Anmeldung Nr:
Application no.: 02360233.7
Demande no:

Anmeldetag:
Date of filing: 05.08.02
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

ALCATEL
54, rue La Boétie
75008 Paris
FRANCE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

M:N path protection

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04J/

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR

M:N Path Protection

Field of the Invention

The invention relates to the field of telecommunications and more particularly to a method and corresponding network element for path protection in a transmission network.

Background of the Invention

Transmission networks serve for the transport of user signals, commonly referred to as tributary signals, in the form of multiplexed transmission signals. A transmission network consists of a number a physically interconnected network elements such as add/drop multiplexers, terminal multiplexers, cross-connects and line equipment. The physical interconnection between two network elements is referred to as a section or link while the route a particular tributary takes through the transmission network from end to end is known as a path. Although in the context of path protection, the term path is commonly also used for a segment of a path, the above specification uses the more appropriate terminology and distinguishes between entire paths (from end to end) and path segments without path termination function. A path is represented by a multiplexing unit like a virtual container (VC-N) with its associated path overhead (POH) in SDH (Synchronous Digital Hierarchy). Conversely, a section is represented by an entire transmission frame like a

synchronous transport module (STM-N) with its associated section overhead (SOH).

A very basic aspect of transmission networks is availability of service. Hence, a transmission network itself or the combination of network and network management needs to provide the means and facilities to ensure sufficient availability. Typically, these network mechanisms are distinguished in protection and restoration. The principle of both is to redirect traffic of a failed link to a spare link. Restoration means network management interaction to determine an alternative route through the network while protection uses dedicated protection resources already available and established in the network for this purpose.

Protection mechanisms are widely used and standardised. For example ITU-T G.841 and G.783 describe several protection mechanisms for SDH networks and G.709, G.798 describe corresponding protection mechanisms for OTNs (Optical Transport Networks).

Section protection refers to the protection of a physical link between two network elements. Known section protection mechanisms include 1+1 MSP (Multiplex Section Protection), 1:1 MSP, 1:n MSP and MS-SPRING (Multiplex Section Shared Protection Ring). 1+1 MSP means that two redundant links are provided between two network elements and that all traffic is permanently bridged to the protection links so that the receiving network element can choose the better of the two received signals. 1:1 MSP means that the protection link can be used for extra traffic that is discarded instantly in the case of a failure of the working link and the protected traffic bridged from the failed working to the protection link. 1:n MSP denotes a protection mechanism where one protection link serves to protect n working links. In the case of a failure, traffic from the failed link is bridged to the protection link. 1:1 MSP, 1:n MSP and MS-SPRING require a protocol to communicate a failure from sink to source and synchronize switch-over. SDH uses K1/K2 bytes in the section overhead (SOH) for this purpose.

Conversely, path protection refers to the protection of a path or a segment thereof. G.783 describes a 1+1 path protection mechanism for SDH, which is known as SNCP (Sub-Network Connection Protection). Like for 1+1 MSP, the protected traffic is permanently bridged to a dedicated protection path. A trail termination function required for path level protection is discussed in ITU-T study group 15 draft G.gps (CD-GPS01). An automatic protection protocol on path level is still under discussion and not yet defined, so that 1:1 or 1:n protection on path level is not possible today.

Thus, existing path protection mechanisms require a 100% spare capacity of resources for protection in the network but allow a very fast masking of the failure in terms of availability, typically in less than 50 ms.

Restoration mechanisms are introduced in network management in order to use the spare resources of a network for traffic protection in a flexible way and therefore to reduce the necessary amount of spare resources in a meshed network.

Restoration mechanisms are more stringent in the usage of spare capacity but however, provide a masking of the failure at a lower speed, typically in the range of a few seconds, as completely new paths through the network need to be established by the network management system after the occurrence of a failure. Therefore restoration is regarded as too slow for many applications.

It is therefore an object of the present invention to provide a more efficient and more flexible protection method on path level which allows masking of a failure within shorter time than known restoration methods while still requiring less spare resources in the network than traditional 1+1 path protection mechanisms do.

Summary of the Invention

These and other objects that appear below are achieved by a method that implements a 1:n or m:n path protection mechanism. Rather than defining a

protection protocol to communicate failures and to synchronize switch-over from active to protection path, use is made of the existing tandem connection monitoring (TCM) function, a forced tandem connection reverse defect indication (TC-RDI), and a tandem connection trail trace identifier (TC-TTI). Preferably, the protection method is combined with background restoration of failed paths via network management to re-establish protection after a failure or to revert protection after a new working path is re-established.

In particular, the protection method according to the present invention includes the following steps to recover traffic after the occurrence of a failure affecting a protected network path. First, at least one protected path segment is provided between a first network element and a second network element and at least one protection path segment is provided as well between the first and second network elements. A tandem connection monitoring function is activated on the protected path segment. The protected paths segment is monitored for failures using a tandem connection monitoring function and upon detection of a failure, the occurrence of this failure is communicated to the far end network element using a defect indication and traffic is bridged from the active to the protection path segment. Upon reception of reverse defect indication in the far end network element, the latter bridges traffic from active to the protection path segment, as well. In the case of more than one protected path segments, the failed path is identified by means of a unique trail trace identifier received on the protection path segment. In the case of several protection path segments, one network node is defined as slave node which has to follow the switch-over initiated by the master node and choose the same protection path segment as the master node. Preferably, a combination of two timers enables return from failure condition to normal operation.

The invention allows very fast recovery from failure and can be implemented as an extension of existing mechnisms, which means little implementation effort and the possibility of a stepwise implementation approach.

Brief Description of the Drawings

Preferred embodiments of the present invention will now be described with reference to the accompanying drawings in which

figure 1 shows a bi-directional m:n path protection according to the invention;

figure 2 shows the occurrence of a unidirectional failure and the actions performed by the terminating network elements to recover traffic;

figure 3 shows an alternative to recover the traffic in the failure condition shown in figure 2;

figure 4 shows the return from the failure condition of figure 2 or 3 to normal operation;

figure 5 shows the occurrence of a bi-directional failure and the actions performed by the terminating network nodes to recover traffic;

figure 6 shows the return from the failure condition of figure 5 to normal operation;

figure 7 shows the situation when the bi-directional failure of figure 5 changes into a unidirectional failure;

figure 8 shows a state diagram for a protection path;

figure 9 to 12 show some exceptional situations and corresponding counter-actions; and

figure 13 shows a alternative solution to forced RDI insertion.

Detailed Description of the Invention

The invention recognizes the need for more efficient but inherently fast protection method on path level in a transmission network. The invention therefore proposes an m:n sub-network connection protection (SNCP), where n working paths are protected by m protection paths ($0 < m \leq n$). An m:n sub-network connection protection is shown schematically in figure 1. The path segment ends are denoted by circles in the figures. A first network element NE1 receives n tributary signals 1N-nN (only first and nth tributary signals are shown), which should be transmitted through a transmission network (not shown) to a far end second network element NE2. A number of n working

path segments 1W-nW are thus established through the network from NE1 to NE2. In order to protect these n working path segments, m protection path segments 1P-mP are established between NE1 and NE2, too. All paths are bi-directional, i.e., traffic is passed in both direction between NE1 and NE2. In each of the two network elements NE1, NE2, a switching matrix connects the tributary I/O signals to the corresponding working path segments. The switching matrices serve also for bridging traffic from the tributary I/O signals to protection path segments in the case of a failure.

The m:n protection implies disjoint routing of the working paths (i.e., the use of different physical paths) as far as possible as well as of the protection path in order to reduce the probability of simultaneous multiple failures within the configuration.

As the working paths obviously cannot be permanently bridged to corresponding protection paths, a communication between sink and source network elements is required to communicate failure conditions, negotiate which protection path segment to use and synchronize switch-over. A basic idea of the present invention is thus to use the existing tandem connection monitoring function specified in ITU-T G.707, G.709, and G.783, which are incorporated by reference herein. Tandem connection monitoring in SDH uses the N1 byte of the path overhead (POH) of the virtual container (VC-4) and creates a 76 byte multiframe that is periodically repeated in the N1 byte. On VC-12 or VC-3 level, the N2 byte is available for this function.

A tandem connection is usually defined on a segment of a path also referred to as trail and exists for the purpose of alarm and performance monitoring. For instance, a tandem connection can be transported over a linked sequence of sections on a transmission path.

In the figures, tandem connection source and sink functions are shown as rotated triangles oriented to either left or right. Triangles pointing in transmit direction denote TC source functions and those pointing in receive direction

are denoted as TC sink functions. Non-intrusive tandem connection monitoring functions are shown by upturned triangles.

According to the present invention tandem connections are created on the working path segments between NE1 and NE2. For instance, a tandem connection TC1 for the working path segment 1W is created between termination point 1N and the switching matrix and monitored at the corresponding point 1W. Preferably, tandem connections are created and monitored on the protection paths 1P-nP, too. It has to be noted that on the protection path segments either the TC termination functions or the non-intrusive TC monitoring functions are activated but not both simultaneously.

Figures 2 to 7 illustrate the activities of the network elements to recover traffic in the case of a failure. All figures show the termination points of the paths and tandem connections functions. All failures shown in the below examples affect the protected path 1W. However, this is without restriction to generality as can be seen by simple renumbering of the paths.

Figure 2 illustrates the behaviour in the case of a unidirectional failure. The occurrence of the unidirectional failure on the path 1W is denoted by field 1. The receive end tandem connection monitoring function in receive end point 1W of network element NE2 detects a fault in the tandem connection created on that path segment. As a consequence action shown in field 2, the monitor forces insertion of a reverse defect indication RDI into the overhead of outgoing transmission signals on path 1W and initiates a bridge in the reverse direction from 1N to 1P. Further, the protection path segment 1P is selected to receive transmission signals for 1N.

In a next step shown in field 3, the tandem connection monitoring function of network element NE1 detects RDI in the received signal. As a consequence action, network element NE1 also bridges traffic from 1N to 1P. However, NE1 may keep its selection of 1W to receive traffic from 1N. Further, NE1 also receives traffic from 1N over protection path segment 1P as the far end network element NE2 has switched a bridged from 1N to 1P and can thus

likewise select 1P for traffic from 1N. As both network elements have chosen the same protection path segment 1P, no corrective measures are necessary (field 4). The switch-over is now complete and traffic from failed path segment 1W restored.

It is important to note that according to the present invention, forced TC-RDI is permanently inserted into the traffic signal as long as the failure on working path segment 1W persists. According to the conventional tandem connection protocol, any RDI would immediately disappear as soon as the traffic is re-established over the protection path segment. Therefore, according to traditional TC protocol, it would not be possible to communicate the status of the failed working path segment 1W from sink to source.

The unique tandem connection trail trace identifier (TC-TTI) is used to identify the bridged traffic on a protection path segment. This is especially important if several protection path segments protect several working path segments and it would thus not be certain which working path segment is bridged to which protection path segment.

Rather than using the TC-RDI, use can also be made of the outgoing defect indication (ODI) of the tandem connection. In this case, the ODI has to be forced to inactive as long as no tandem connection defect is detected and forced to active when a tandem connection defect is detected. The use of ODI rather than TC-RDI has the advantage that the far end performance monitoring data is not disturbed.

The fault conditions for the tandem connection monitor can be any of the following failures:

TC-SSF tandem connection server signal fail, i.e., the next higher server layer has already failed, SSF is thus generated to prevent misleading alarms at lower layers.

TC-UNEQ tandem connection unequipped, i.e., no tandem connection information is received.

TC-TIM tandem connection trail trace identifier mismatch, i.e., a wrong TC-TTI is received.

TC-LTC loss of tandem connection, i.e., a tandem connection signal is received but the TC multiframe is faulty and cannot be evaluated.

Figure 3 shows the situation where network element NE1, responsive to detecting RDI on the failed path segment 1W, has chosen a different protection path segment mP. This can happen in the situation where no protection path segment already contains tandem connection information TC1 from 1N. Therefore, correction of the switch over is necessary. Network element NE1 on the left hand side is defined as slave while network element NE2 on the right side is defined as the master. Network element NE1 detects tandem connection TC1 from failed path segment 1W at protection path segment 1P. As slave network element, it has to follow the decision of network element NE2 and reconfigures its bride 1N-nP to 1N-1P and selects 1P to receive traffic for 1N.

At the same time, network element NE2 on the far end side detects tandem connection information TC1 from 1W in mP, which was initially chosen by network element NE1. However, because network element NE2 is defined as master, it keeps its bridge to and selection of 1P.

Figure 4 shows the return to normal operation after repair of the unidirectional failure. Field 1 indicates that the unidirectional failure has been cleared. In a first step (field 2), tandem connection monitoring function for path segment 1W in network element NE2 detects that the tandem connection fault is cleared and valid tandem connection information is received. As a consequence action, the forced RDI insertion is removed. As no tandem connection RDI is received and no TC fault is detected anymore on 1W, a first timer, which is called WRS (Wait to Revert Selection), is started (field 3). At the same time, network element NE1 detects at its tandem connection monitoring function for 1W that no TC-RDI is received anymore (field 4). As there is no fault condition for 1W, it starts its first timer WRS, too.

After the WRS timer in network element NE2 expires, path segment 1W is selected for 1N and a second timer called WRB (Wait to Remove Bridge) is started (field 5). At about the same time, WRS timer in network element NE1 expires as well (field 6) and network element NE1 selects if necessary 1W again as active path segment for 1N and starts its second timer WRB.

After the WRB timer in network element NE2 expires, NE2 removes the bridge from 1N to 1P (field 7). At about the same time, WRB timer in network element NE1 expires as well (field 8) and NE1 removes its bridge from 1N to 1P as well and return to normal operation is complete.

Figure 5 shows the occurrence of a bi-directional failure (field 1) on active path segment 1W. The tandem connection monitoring functions in both network elements detect a fault condition and force insertion of TC-RDI, bridge 1N to a protection path segment and select this protection path segment for receiving traffic for 1N (field 2). The selection of the protection path segment is random in the first step. As shown, network element NE1 selects and bridges to protection path segment mP while network element NE2 selects and bridges to 1P. As the selected protection paths segment do not match, corrective measures are necessary. Network element NE1 is defined as slave, while network element NE2 is defined as master. Therefore, network element NE1, as it detects tandem connection information TC1 for path 1N on protection path segment 1P, reconfigures its selection to 1P and shifts the bridge from 1N-mP to 1N-1P. Conversely, network element NE2 detects tandem connection information TC1 on protection path segment mP but does not reconfigure its protection switching as it is defined as master network element, i.e., not to track the switch decision of the far end side. Protection switching is thus established and traffic from protected path 1N restored.

Figure 6 shows the return to normal operation after the bi-directional failure of figure 5 has been repaired. Field 1 indicates that the bi-directional failure has been cleared. Both network elements detect that the tandem connection fault condition has disappeared (field 2) and clear their forced TC-RDI insertion. Then they both start their WRS timer (field 3).

After the WRS timer in network element NE2 expires, path segment 1W is selected for 1N and a WRB timer is started (field 4). At about the same time, WRS timer in network element NE1 expires as well (field 5) and network element NE1 also selects 1W as active path segment to receive traffic for path 1N and starts its WRB timer.

After the WRB timer in network element NE2 expires, NE2 removes the bridge from 1N to 1P (field 6). At about the same time, WRB timer in network element NE1 expires as well (field 7) and NE1 removes its bridge from 1N to 1P as well and return to normal operation is complete.

Figure 7 shows what happens in the case when the bi-directional failure is repaired in only one direction and thus changes into a unidirectional failure (field 1). Network element NE2 detects that the tandem connection fault condition does no longer exist and clears its forced TC-RDI insertion (field 2). But as it still receives TC-RDI from network element NE1 on path segment 1W, it does not initiate return to normal operation and keeps selection of path segment 1P and bridge from 1N to 1P active. Reversion is started only when both directions of 1W are okay, i.e., when there is no TC-RDI anymore in either direction.

A state diagram for a protection path is presented in figure 8. It contains the following states:

FAILED This state is entered if in the IDLE state the TC(P) sink or during PENDING/PROTECTING/WRB/WRS the TC(P) monitor has detected a TC-Fault (=TC-SSF, TC-UNEQ, TC-TIM or TC-LTC) or TC-RDI. TC-TIM is only considered if it does not match to any TC-TTI defined for the working paths. P is continuously monitored with a TC(p) sink/source function. N.B. during protection there will be an sctive TC-TIM alarm and forced inserted TC-RDI is not reported by TC(p) because the TIM alarm suppresses TC-RDI.

IDLE xP is idle and supervised with TC(P) (sink/source) and there is no TC-Fault or TDC-RDI.

PENDING xP is selected to protect yW. The normal path (yN) is bridged to xP and xP is selected. In case yW detects a TC-Fault the TC source at yN is forced to insert TC-RDI. The far end NE has not yet initiated the protection. N.B., yW shall be selected if it is only in TC-RDI.

PROTECTING xP protects yW. The normal path (yN) is bridged to xP and xP is selected. In case yW detects a TC-Fault, the TC source at yN is forced to insert TC-RDI.

WRS Wait to Reverse Selector, yW ok, bridge to xP, xP selected.

WRB Wait to Remove Bridge, yW ok, bridge to xP, yW selected.

The following events are considered in figure 8:

Signal Events

W ok TC-Faults and TC-RDI cleared (transition 'W nok' -> 'W ok')

W nok TC-Fault or TC-RDI detected (transition 'W ok' -> 'W nok')

P ok No TC-Fault and no TC-RDI detected.

P nok TC-Fault or TC-RDI detected. TC-TIM is only considered if it does not match to any TC-TTI defined for the working paths. A TC-TIM alarm suppresses TC-RDI, e.g., when the other side has bridged a working channel (this would lead to TC-TIM for the TC(P) and is forcing insertion of TC-RDI; this TC-RDI would not be detected and P would still be ok).

Identification Events

W identified in P Signal from path segment W is identified in path segment P

W not identified in P Signal from path segment W is not identified in path segment P

W identified in P* while path segment W is being bridged to path segment P, signal from path segment W is identified in path segment P*

Tim r Events

WRB, WRS exp. WRB, WRS timer function expired.

The table at the end of the specification shows an event / state check for the state diagram in figure 8.

Figure 9 shows the exceptional situation when an external tandem connection interferes with the tandem connection created on the protected path segment. This situation may occur especially in SDH networks since SDH allows only one level of tandem connections while nested or overlapping tandem connections are not permitted. Therefore, this situation is regarded as faulty and protection switching is initiated as for a bi-directional failure (see figure 7).

In figure 9, network element NE2 detects a failure condition TC-UNEQ (tandem connection unequipped) on path segment 1W, i.e., it receives no tandem connection information as the TC signal inserted by network element NE1 is terminated by the faulty tandem connection sink function on the path segment 1W. Therefore, it initiates protection switching as in figure 7.

Network element NE1 probably detects TC-TIM (tandem connection trail trace identifier mismatch), depending on the TC-TTI (trail trace identifier) used in the external tandem connection. In this case, NE1 also initiates protection switching as in figure 7.

Figure 10 shows the situation when an intermediate network element has opened the connection, for example in its switching matrix. Field 1 denotes an open matrix in an intermediate network element. Both terminating network elements thus receive and detect an unequipped tandem connection signal (field 2) and initiate path protection as for a bi-directional failure.

Figure 11 shows the exceptional situation when a protection segment fails during protection, i.e., path 1N is bridged due to a failure on working path segment 1W to protection path segment 1P and 1P fails as well. In this event,

both network elements NE1 and NE2 detect a tandem connection fault condition. The protection path segment 1P thus enters into FAILED state and a new protection is initiated for protected path segment 1W, excluding path segment 1P from the protection.

Figure 12 shows the situation that the idle protection path segment 1P fails (unidirectional failure). At network element NE2, the monitoring function for a tandem connection created on the protection path segment 1P detects a TC fault condition. Path 1P goes thus in FAILED state and network element NE2 automatically inserts TC-RDI in reverse direction. Monitoring function in network element NE1 detects no fault condition but TC-RDI on path segment 1P and thus also goes in FAILED state for path segment 1P. 1P is thus excluded from the protection and will, as long as the failure persists, not be used in the case that one of the working paths segment fail.

An alternative to forced RDI insertion as in the above embodiments is shown in figure 13. After occurrence of a bi-directional failure on path segment 1W (field 1), network element NE2 detects the TC fault condition. As a consequence action, NE2 creates a new tandem connection on failed path segment 1W by duplicating the existing tandem connection TC1 and bridges traffic from 1N to segment 1P and selects 1P to receive traffic for 1N (field 2). The duplicated TC1 will automatically insert RDI in reverse direction due to the occurrence of the failure. Network element NE1 therefore detects either a TC fault condition or the RDI inserted by duplicated TC1. As a consequence action, it also duplicates the tandem connection TC1, bridges 1N to 1P and selects 1P. If both network elements have selected the same protection path segment 1P, no corrective measures are necessary. Otherwise, a re-configuration of the protection switch by NE1 defined as slave would be initiated as explained above. The duplicated tandem connection TC1 on 1W serves to detect when the failure is removed in order to initiate return to normal operation.

This alternative makes use of the fact that according to conventional TC protocol, RDI is generated as long as a path segment on which the tandem

connection is created fails. However, due to the protection switching, the overall path from 1N to 1N would be re-established over the protection path segment 1P and RDI on TC1 would thus automatically disappear. The alternative embodiment now shifts the duplicated TCM function TC1 from behind the switching matrix to in front of the switching matrix. This way, the failed path segment from 1W to 1W is exclusively monitored by the duplicated TC1 and RDI is sent on the duplicated TC1 as long as the failure persists. This allows to communicate the status of the failed working path segment from sink to source using TC-RDI without any modification to the existing TCM protocol, i.e., without introducing a forced RDI insertion function.

In a preferred improvement of the present invention, a network restoration is performed by the network management system in the case of a failure in order to establish a new path segment for the used protection path. The purpose is to restore the initial protection configuration (M:N) by providing a new working path from the available resources in the network. After the new path segment is re-established, reversion from protection may be initiated as explained above.

The network manager may consider path priorities and pre-emption for restoration, however, this does not necessarily mean that the NEs have to consider different priorities within the m:n paths during protection switching. Nonetheless, a further improvement of the present invention may consist in providing the ability to take into account different priorities of the protected paths for protection switching. For instance, an already established protection for a protected path of lower priority may be discarded to recover traffic of a failed protected path with higher priority. In a further improvement, idle protection paths may carry extra traffic.

One main reason to introduce m:n protection is the fast response time on failures. A preferable architecture would be to control the m:n protection switching in the central NE control instance, because inherently several I/O boards will be involved in an m:n configuration. However, large transmission network elements such as crossconnects may be composed of a number of

I/O and matrix boards installed in several shelves, each having its own shelf controller that communicates with and is controlled by the central NE controller. In this case, data communication architecture between shelf controllers and central NE controller may not allow to perform the switching in the required response times of for example less than 300 ms.

There are several possible solutions to solve this problem. On the one hand, a real-time communication between the shelf controllers and a NE-central protection control unit can be implemented. On the other hand, a real-time data communication between the shelf controllers may be provided in order to synchronise protection switching between the shelf controllers. And further, protection switching may be implemented in the shelf controllers with the restriction that all working and protection paths of one m:n protection group must be routed to one shelf of the terminating NEs.

Although the invention has been explained for a segment of a path, it is clear, that the invention would be equally applicable to the protection of entire paths.

Eur päisches Patentamt	European Patent Office	Office européen des brevets

Q760026
1581

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. | Patent application No. | Demande de brevet n°

02360233.7

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Network Protection and OA&M mechanism for WDM Optical Path Transport Networks

Satoru Okamoto, Atsushi Watanabe, Naohide Nagatsu, and Ken-ichi Sato

NTT Optical Network Systems Laboratories
1-1 Hikari-no-oka, Yokosuka-shi, Kanagawa, 239-0847, Japan

Abstract To realize a large scale and robust photonic transport network, this paper proposes a network protection strategy and maintenance signaling flow for WDM optical path transport networks. The network protection strategy is applicable for mesh-type WDM optical path transport networks, and the OA&M flow that is required for the network to recover from failures are clarified. The proposed OA&M flow does not rely on the OP-AIS (optical path alarm indication signal) generation method. This signaling method can also be applied to the all-optical type network.

1 Introduction

The optical path (OP) concept based on WDM (Wavelength Division Multiplexing) technologies has been proposed [1, 2] and the necessary technical developments to embody it have been realized [3, 4]. From the network management viewpoint, establishment of the network protection strategy and OA&M (operation administration and management) technologies are important to construct robust WDM optical path transport networks.

This paper proposes a network protection strategy for mesh-type WDM optical path transport networks and the OA&M flow that is required for the network to recover from failures. The proposed OA&M flow does not rely on the OP-AIS generation principle, although the same result is achieved with an OP-AIS insertion method.

2 Overview of Optical Path Transport Networks

The network discussed in this paper is based on the wavelength routing [5] technology. The optical path is defined in the path layer since wavelength routing will be done in the optical path layer using optical path cross-connects (OPXCs), and the optical paths can be utilized for network restoration as in the existing electrical path restoration scheme [6]. Therefore, the optical path network can provide a base that is failure resilient and allows for smooth evolution of client electrical signal transfer technologies (cell-based ATM etc.) which is attained by maximally exploiting optical transparency. Optical path benefits from the network architecture viewpoint are shown in [6–8].

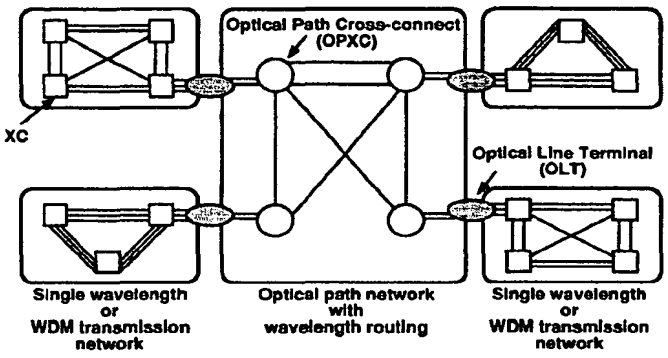

Figure 1: Application example of the WDM optical path transport network.

Figure 1 shows an example of optical path network application. The optical path network interconnects single wavelength or WDM transmission networks. As one example, these single wavelength or WDM transmission networks may correspond to regional transport networks while the optical path network will be applied to a nationwide backbone network. Optical paths are assigned between two optical line terminals (OLTs); electrical paths (SDH VC-4s, VC-4-16c, ATM VPs, etc.) are accommodated into optical paths. Each optical path will, in most cases, offer 2.5Gbps or 10Gbps capacity (of course not restricted to those values) to maximally exploit the benefits of optical transmission.

3 Functional Architecture Model

This section presents the WDM optical transport network functional architecture model by using the NE (network element) connection model. The detailed layered architecture and allocated functions are discussed in other papers [8–13].

3.1 Optical layer definition

The transport network layered architectures of the existing SDH network defined in G.803 [14], the SDH-based ATM network defined in I.311 [15], and the newly proposed SDH-based optical path network [9, 10] are depicted in Fig.2. There are some differ-

0-7803-4788-9/98/$10.00 © 1998 IEEE.

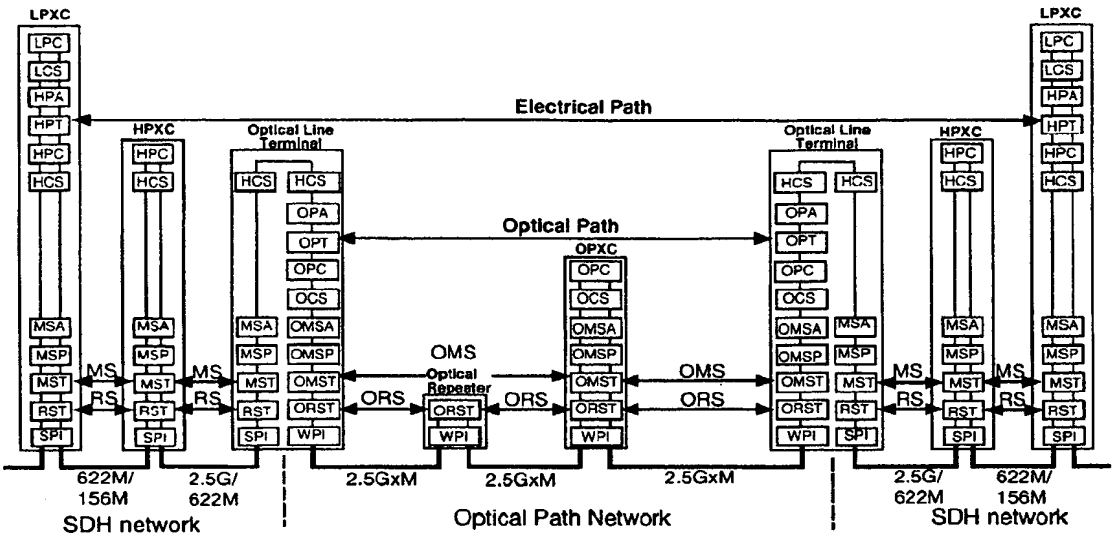

Figure 3: Network element connection model. LPXC : lower order path cross-connect, HPXC : higher order path cross-connect

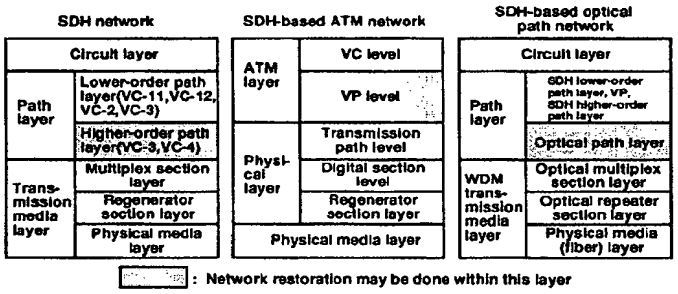

Figure 2: Transport network layered model.

ences between the SDH and ATM network architectures, but the important point is that maximum commonality is retained. The proposed SDH-based optical path network layered architecture also needs maximum commonality with existing SDH networks. This is because exploiting the already established SDH technologies realizes the economical introduction of optical paths with minimum delay and maximum efficiency through the utilization of SDH network operation capabilities.

An optical path layer is introduced in the path layer. Therefore, the path layer has two sub-layers: an electrical path (EP) layer and an optical path (OP) layer. The important characteristic for optical path layer introduction is that the optical path layer is a server layer of the SDH higher order path layer; several SDH paths are directly accommodated into each optical path. This is one of the major difference from the WDM transmission network discussed in G.681 [16] which accommodates section layer signals such as the SDH STM-N into an optical channel.

The WDM transmission media layer is composed of an optical multiplex section (OMS) layer, an optical repeater section (ORS) layer, and a physical media (i.e. optical fiber) layer. The OMS layer is concerned with the end-to-end transfer of information between locations that transfer or terminate optical paths whereas the ORS layer is concerned with the transfer of information between individual optical repeaters. Optical repeaters can be either linear repeaters (L-REPs [17]) or non-linear repeaters (nL-REPs).

The optical layer is defined as consisting of the optical path layer and the optical section layer.

3.2 NE connection model

The optical path network architecture supporting SDH is described by the NE connection model depicted in Fig. 3. Here, one electrical path (HOP : SDH higher order path) trail transported with optical paths is described for simplicity. This HOP is terminated at lower order path cross-connect systems (LPXCs). The server layer of each HOP connection is the multiplex section (MS) trail in the SDH transport network or an optical path (OP) trail in the WDM optical path transport network.

Optical paths are terminated at the optical line terminals (OLTs). The OPA (opticap path adaptation) function performs network-to-network interfacing. In this example, the OLT converts the SDH signal format to the optical path signal format and vice versa. This signal format conversion is easily implemented by already developed SDH section layer processing LSIs [8]. Therefore, the most cost-effective OP transport network introduction is possible.

4 WDM Optical Path Transport Network Protection Strategy

The layered network concept produces a significant characteristic; independence between layers. This means that each layer can have own network protection system. It is necessary, therefore, to construct the most effective network protection system in terms

Table 1: Possible network protection strategies.

Layer	Implementation	Remarks
Electrical path (ex. HOP, VP)	possible	Restoration/protection. Effective resource utilization.
Electrical section (ex. MS)	impossible (no MS layer)	Fast protection (<50ms) is required in SDH networks.
Optical path	possible	Restoration/protection. 1+1 and 1:n protections are possible.
Optical section (ex. OMS)	possible	1+1 or 1:n protection

of resource utilization and restoration time. Important key words are "escalation" and "redundancy".

Possible network protection schemes are OMS protection in the OMS layer, OP protection/restoration in the OP layer, MS protection in the SDH MS layer, HOP protection/restoration in the SDH HOP layer, and VP protection/restoration in the ATM VP layer. In the existing SDH transport network, layer escalation, in which MS protection is attempted before HOP restoration, has been implemented. Therefore, protection time of MS protection must be short, say, less than 50ms, and few seconds of guard time is added before HOP restoration is activated.

A multi-layer protection scheme requires a tremendous amount of spare resources. This is because 1+1 protection requires 100% spare resources. Two layer protection scheme requires 200% and three layer protection scheme requires 400% spare resources in the network.

Possible protection implementation candidates for the WDM optical path network are summarized in Table 1.

4.1 Network protection examples for WDM OP mesh-type networks

As shown in Table 1, MS protection is not applied in WDM optical path transport networks. Because SDH MS layer is not the client of the OP layer; see Fig. 3. Instead, as mentioned in section 2, OP restoration/protection is an effective network protection scheme. The client layer of the optical path layer is the electrical path (EP) layer. Therefore, co-operation between the EP restoration/protection and the OP restoration/protection or the layer escalation from the OP layer to the EP layer should be implemented. As shown in Fig. 3, electrical paths (SDH HOPs: VC-4s) lie across the WDM optical path transport network and SDH transport network. All SDH networks adopt escalation from MS protection to HOP restoration, if HOP restoration is implemented. Therefore, in the case of escalation from OP restoration/protection to HOP restoration, the processing speed requirement for OP restoration/protection is the same as that for MS protection. This is not easy to achieve in the case of the OP restoration. To solve this problem, we propose utilize a network partitioning principle with the tandem connection concept [8]. Figure 4 shows an example of the proposed network partitioning. The VC-4 trail shown in Fig.4 lies across the SDH transport networks and the WDM optical path transport network. In each transport network, the VC-4 sub-network connection can be defined and each VC-4 sub-network connection is managed as a VC-4 tandem connection (TC). The VC-4 trail is partitioned into VC-4 TCs. The VC-4 TC on the WDM optical path transport network has no restoration function, because there are no SDH NEs in the optical path network. Therefore, restoration of the VC-4 trail is performed by optical path trail restoration in the WDM optical path transport network. On the other hand, in the SDH transport network, restoration is performed by VC-4 TC level restoration, and by multiplex section (MS) trail protection in network-to-network connection links. The same concept is being discussed regarding ATM networks in ITU-T [18]. In the ATM world, the tandem connection is called a "protected domain".

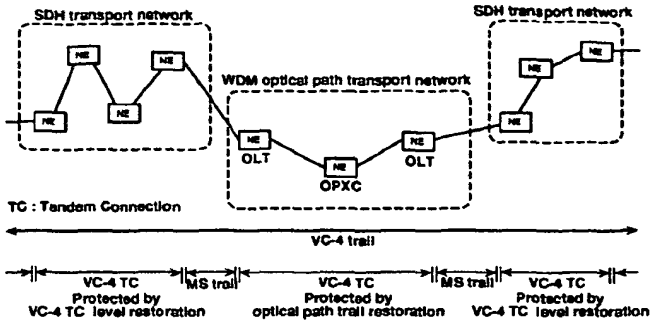

Figure 4: VC-4 trail transported via tandem connections.

Introduction of network partitioning and the tandem connection concept enables efficient multi-operator domain trail management. A comparison of the layer escalation concept and the tandem connection concept based network protection scheme is discussed in the next section.

The OMS protection scheme is also applicable to WDM OP mesh-type networks. Consideration is, however, needed of the topological restriction that often occurs, i.e., route diversity is difficult. In this case, if route failure occurs, both working and protection OMS trails will be damaged and OMS protection can not be activated. Therefore, the OMS protection scheme is not always effective in this type of network. OP restoration and OP protection are the most effective network protection schemes in mesh-type WDM optical path transport networks.

4.2 OP restoration scheme

As described in the above section, the OP restoration scheme is divided into two types. One is the escalation type, the other is the tandem connection, i.e., no escalation type.

Figure 5(a) shows a layer escalation type network protection example. When a failure occurred, OP restoration is first activated. If OP restoration is not successful, then SDH HOP restoration is activated. In this example, the backup SDH HOP is required. This HOP is a backup path in the SDH HOP layer. However, in the OP layer, two working OPs should be prepared, one for the working SDH HOP and the other for the backup SDH HOP, because of the layer independence. This means that backup

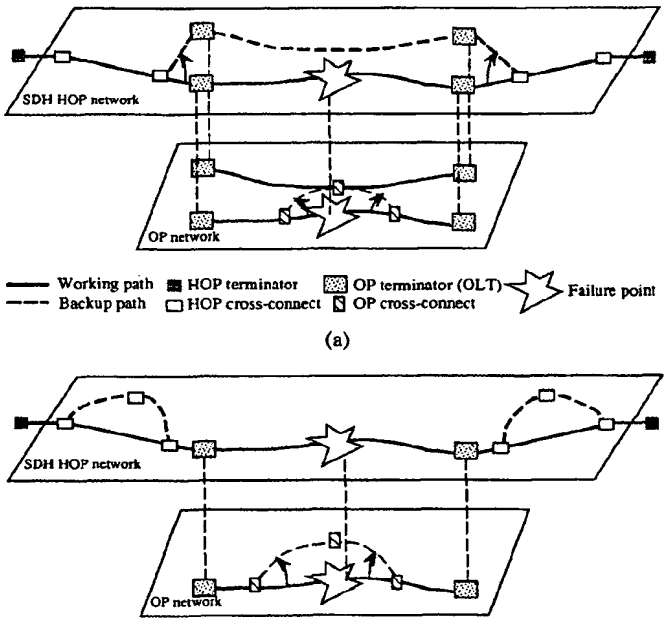

Figure 5: Network protection implementation of the WDM optical path transport network system. (a) Layer escalation type (OP restoration to HOP restoration). (b) Tandem connection type.

OPs are required for both working and backup SDH HOPs.

Figure 5(b) shows a tandem connection type network protection example. Backup HOPs are set up only in the SDH transport network area. Therefore, network resources requirements can be reduced.

4.3 Hitless protection scheme

Some kinds of leased line services require hitless protection switching or "minimum services down" switching for failure recovery. This can be realized by a diversity routing technique. A protected HOP is set up between two HOP terminators. At the HOP cross-connect, which is located at the HOP network entrance point, the protected HOP is diverted to two route-independent HOPs. At the receiving side HOP cross-connect, the signal phase of the two HOPs is adjusted by using an elastic store memory. When a failure occurs, protection switching is only performed in the receiving side HOP cross-connect node. Thus, hitless protection or "minimum service down" service is possible on the protected HOP.

The layer escalation type hitless protection implementation example is shown in Fig. 6(a). For diverted working HOPs and the backup HOP, three corresponding working OPs and the backup OPs are required. This requirement for network resource redundancy can be reduced if the network planning system grasps all the information about all layer networks. This is, however, against why the layering concept and partitioning concept were

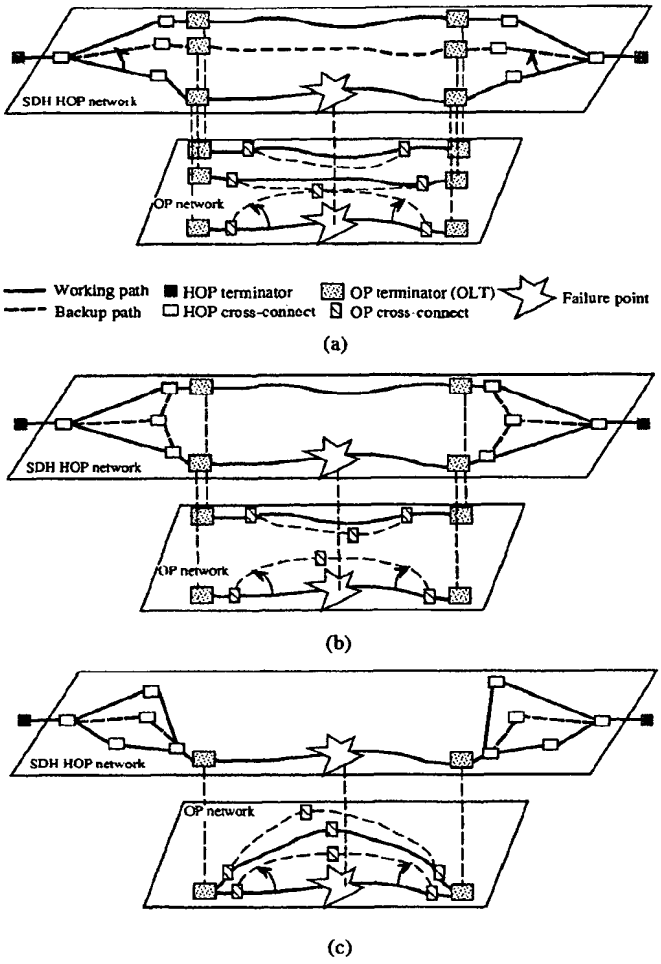

Figure 6: Hitless protection implementation. (a) Layer escalation type. (b) Tandem connection type-1. (c) Tandem connection type-2 (OP hitless protection type).

added to the transport network architecture – to simplify network operation and to enable each layer to evolve independently from other layers.

Tandem connection type hitless protection implementation examples are shown in Fig. 6(b) – type-1 and (c) – type-2. In the case of type-1 implementation, a relatively relaxed version of the tandem connection concept is applied. Backup HOPs are set up only in the SDH transport network area. In the OP network area, it is essential that the HOP pair is accommodated so that no common routes are assigned for each one of the pair and no OPXCs are shared. This also weakens the idea of layer independency. However, it can be a very practical approach. Type-2 implementation strictly follows the tandem connection concept. The HOP pair is set up only in the SDH transport network area. In the OP network, OP hitless switching is performed at OLT. This is the best approach from the logical viewpoint. However, the cost of OP hitless protection implementation and system reliability of

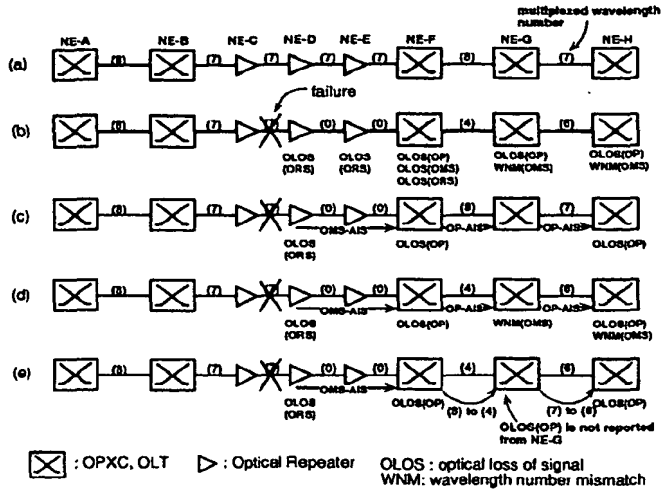

Figure 7: Maintenance signal flow examples. (a) Normal operation state. (b) No OMS-AIS and no OP-AIS state. (c) OMS-AIS(in overhead) insertion and OP-AIS insertion case. (d) OMS-AIS(in overhead) insertion and OP-AIS(in overhead) case. (e) OMS-AIS(in overhead) insertion and no OP-AIS state.

non-protected OLT should be evaluated before applicability can be determined.

5 OA&M flow in The WDM Optical Transport Network

When failure occurs, a network element should detect a fault and generate maintenance signals to indicate the unavailability of the trail(s) to other NEs. In the existing SDH network, RDI (remote defect indication) and AISs (alarm indication signal), such as MS-AIS, AU(TU)-AIS, and VC-AIS [19] are sent upstream and downstream, respectively, to identify the unavailable section and path after fault detection. In the SDH case, all "1"s in the entire STM-N, AU(TU)-n, and VC-n, excluding the valid overhead region are generated for AIS. The insertion of AIS has two important features. One is fault notification to the trail termination point, the other is to suppress fault detection at intermediate NEs.

In the WDM optical transport network, OMS-AIS and OP-AIS are required to operate the network. To realize all "1"s or dummy signal insertion, optical senders are required in all NEs. This is not practical in WDM optical transport networks, especially in all-optical networks. Therefore, the overhead channel should be used to notify the AIS to downstream NEs. This is a practical approach for OMS-AIS because a separate wavelength channel can be used for the optical section overhead channel. On the other hand, the optical path overhead channel needs to be transferred with the payload channel [8, 13]. It is difficult to transfer AIS over the optical path overhead channel because both the OP payload channel and the OP overhead channel are lost.

If AIS is not transferred to downstream NEs, all NEs detect the failure and many alarms are generated and notified to the network OpS (operation system). This is depicted in Fig. 7(b). When failure occurs between NE-B and NE-C, OLOS (optical loss of signal) in the ORS layer is detected at NE-D, NE-E, and NE-F. At NE-F, OLOS in the OMS layer and OLOS in the OP layer are also detected. In this case, it is assumed that the number of multiplexed wavelengths between NE-F and NE-G is changed from eight to four, between NE-G and NF-H is changed from seven to six, respectively. Therefore, WNM (wavelength number mismatch) in the OMS layer is detected at NE-G and NE-H. OLOS in the OP layer is also detected at NE-G and NE-H.

The ideal case is shown in Fig. 7(c). OP-AIS can be inserted into the OP payload channel. OLOS in the OMS layer is suppressed by OMS-AIS in the optical section overhead channel. WNM in the OMS layer and OLOS in the OP layer at NE-G are suppressed by OP-AIS indicated in the OP payload channel.

When an OP-AIS is transferred with the OP overhead channel, WNM in the OMS layer is detected at NE-G and NE-H; see Fig. 7(d).

The proposed mechanism is described in Fig. 7(e). The most important point is that OP-AIS is not utilized in this mechanism. Two actions characterize this OA&M flow.

ACTION-1 : OMS is reconfigured by notifying the multiplexed wavelength number from the upper NE to downstream NE. When OLOS in the OP is detected, first, the NE management system looks up the output OMS indicated in the OP connection matrix table. Next, the changed multiplexed wavelength number is calculated and the NE management system notifies the downstream NE by using the OMS overhead.

ACTION-2 : OLOS in the OP layer is reported to the OpS when following conditions are fulfilled. a) OLOS is detected and b-1) OMS fault condition continues, or b-2) OP is terminated in this NE, or b-3) equipment failure is detected in this NE.

In case of Fig. 7(e), OLOS in the OP layer is detected at NE-F, NE-G, and NE-H. ACTION-1 is activated at NEs, so WMN alarm at NE-G and NE-H are released. As a result, when ACTION-2 is executed at NEs, OLOS alarms are reported from only NE-F and NE-H. This result is the same as that of the ideal case (Fig. 7(c)). To implement ACTION-1 and ACTION-2, the timing sequence including processing time and guard time should be determined. If OP-AIS is used with the proposed method, more rapid timing sequence may be achieved. However, the proposed mechanism can be applied to all WDM optical transport networks which do not implement an OP-AIS mechanism.

6 Conclusion

This paper proposed an efficient network protection mechanism and the OA&M flow for WDM optical path transport networks.

The multi-wavelength network and the single wavelength network will have different network protection and restoration methods. Therefore, the coordination and cooperation of these methods are necessary. The tandem connection (in SDH) and the protected domain (in ATM) approach solves operational problems. The proposed network protection method is based on a combination of both the layered network concept and the network partitioning concept. Large-scale, large capacity, robust, and easily operated WDM optical path transport networks can be developed by applying the proposed method.

The OA&M flow of the failure notification was also discussed. The proposed OA&M flow does not rely on the OP-AIS generation method. Therefore, the proposed signaling method can also be applied to the all-optical type networks.

References

[1] K. Sato, S. Okamoto, and H. Hadama, "Optical path layer technologies to enhance B-ISDN performance," Proc. IEEE ICC '93 (Geneva, Switzerland), pp.1300–1307, May 1993.

[2] K. Sato, S. Okamoto, and H. Hadama, "Network performance and integrity enhancement with optical path layer technologies," IEEE JSAC, vol. SAC-12, no.1, pp.159–170, Jan. 1994.

[3] S. Okamoto, A. Watanabe, and K. Sato, "Optical path cross-connect node architectures for photonic transport network," IEEE JLT, vol.14, No.6, pp.1410-1422, June 1996.

[4] M. Koga, A. Watanabe, S. Okamoto, K. Sato, and M. Okuno, "8×16 delivery-and-coupling-type optical switches for a 320-Gigabit/s throughout optical path cross-connect system," Proc. OFC '96, San Jose, California, February 25-March 1, 1996, ThN3.

[5] G. R. Hill, "A Wavelength Routing Approach to Optical Communication Networks," Proc. IEEE INFOCOM '88, pp.354-362, 1988.

[6] K. Sato, "Photonic transport network OAM technologies," IEEE Communications Magazine, pp.86–94, Dec. 1996.

[7] K. Sato, S. Okamoto, and A. Watanabe, "Photonic transport networks based on optical paths," International Journal of Communication Systems Vol.8, no. 4, pp.377-389, 1995.

[8] S. Okamoto and K. Sato, "Inter-network interface for photonic transport networks and SDH transport networks," Proc. IEEE GLOBECOM '97 (Phoenix, AZ, USA), pp.850–855, Nov. 1997.

[9] S. Okamoto, N. Nagatsu, K. Oguchi, and K. Sato, "Management concepts of optical path networks," ICC'95 Workshop on WDM optical network management and control, Seattle, USA, 18-22 June 1995, Paper #3, pp.19-26.

[10] S. Okamoto, K. Oguchi, and K. Sato, "Network architecture and management concepts for optical transport networks," Proc. NOMS'96, Kyoto, Japan, 15-19 April 1996, pp.1-11.

[11] S. Okamoto, K. Oguchi, and K. Sato, "The layered architecture of optical transport networks," Proc. 1996 IEICE general conference, Tokyo, Japan, 28-30 March 1996, B-1145.

[12] S. Okamoto, K. Oguchi, and K. Sato, "Layered architecture of WDM networks employing optical paths," ICC'96 Workshop on WDM optical network management and control, Dallas, USA, 23-27 June 1996, Paper #4.

[13] S. Okamoto, K. Oguchi, and K. Sato, "Network architecture for optical path transport networks," IEEE COM, vol.45, No.8, pp.968–977, August 1997.

[14] ITU-T Recommendation G.803, "Architectures of transport networks based on the synchronous digital hierarchy (SDH)," March 1993.

[15] ITU-T Recommendation I.311, "B-ISDN general network aspects," March 1993.

[16] ITU-T Draft Recommendation G.681, "Functional characteristics of interoffice and long-haul line systems using optical amplifiers, including optical multiplexing," June 1996.

[17] Y. Kobayashi, Y. Sato, K. Aida, K. Hagimoto, and K. Nakagawa, "SDH-based 10 Gbit/s optical transmission system," Proc. IEEE GLOBECOM '94 (San Francisco, USA), pp.1166–1170, Nov. 1994.

[18] ITU-T SG 13 Q.6 Meeting, Seoul, Korea, 17-28 Feb. 1997, "Proposed VP/VC protection switching method," Working Document No. D.43(WP3/13), Source: NTT.

[19] ITU-T Draft Recommendation G.707, "Network node interface for the synchronous digital hierarchy," March 1996.

What is claimed is

1. A method for sub-network connection protection in a transmission network, said method comprising the steps of:

- providing at least one protected path segment (1W) between a first network element (NE1) and a second network element (NE2);
- providing at least one protection path segment (1P) between said first and second network elements (NE1, NE2);
- creating a tandem connection (TC1) along said protected path segment (1P) between said first and second network elements (NE1, NE2);
- detecting a failure on said protected path segment (1W) by means of a tandem connection monitoring function in the second network element (NE2); and
- upon detection of the failure; inserting a tandem connection defect indication (RDI) into a reverse traffic signal, bridging said reverse traffic signal to the protection path segment (1P), and selecting said protection path segment (1P) to receive a traffic signal from the protection path segment (1P), wherein said defect indication (RDI) being transmitted on the protected path segment at least as long as the failure persists.

2. A method according to claim 1, further comprising the step of:

- upon reception of said defect indication (RDI) at the first network element (NE1), bridging said traffic signal to the protection path segment (1P).

3. A method according to claim 1, further comprising the steps of:
- detecting said failure by means of a tandem connection monitoring function in the first network element (NE1); and
- upon detection of the failure; inserting a defect indication (RDI) into said traffic signal, bridging said traffic signal to a protection path segment (mP), and selecting said protection path segment (mP) to receive said reverse traffic signal from the protection path segment (mP).

4. A method according to claim 1, wherein the insertion of said defect indication (RDI) being effected by a forced insertion that persists even after traffic has been re-established over said protection path segment (1P) as long as the failure on the working path segment (1W) persists.

5. A method according to claim 1, wherein the insertion of said defect indication (RDI) being effected by creating a duplicated tandem connection termination function in front of the switching point for the bridge, so that said duplicated tandem connection termination function serves for exclusively monitoring said failed protected path segment (1W) and automatically inserting a reverse defect indication (RDI) as long as the failure persists.

6. A method according to claim 1, further comprising the steps of assigning an unique trail trace identifier to said tandem connection on said protected path segment and identifying a bridged traffic signal on a protection path segment by means of said trail trace identifier.

7. A method according to claim 1, further comprising the step of defining one of the tandem connection terminating network elements (NE1, NE2) as slave network element (NE1) and the other as master network element (NE2), said slave network element following the selection of a protection path segment of the master network element and using the same selected protection path segment in the case of a failure.

8. A method according to claim 1, further comprising the step of detecting when said failure is no longer present or when said defect indication is no longer received and initiating revert to normal operation.

9. A method according to claim 8, further comprising the steps of starting a first timer (WRS); after lapse of said first timer, reverting selection of said protection path segment and starting a second timer (WRB) and after lapse of said second timer, removing said bridge to said protection path segment.

10. A method according to claim 1, further comprising the steps of:
- communicating the occurrence of the failure to a network management system; and
- by means of said network management system, providing a new working path segment between said first and second network elements.

11. A method according to claim 1, wherein said tandem connection defect indication is a tandem connection reverse defect indication or a tandem connection outgoing defect indication.

12. A method of protecting at least one protected path segment (1W) between a first network element (NE1) and a second network element (NE2) in a transmission network by means of at least one protection path segment (1P), said method comprising the steps of detecting a failure on said protected path segment (1W) and bridging a traffic signal (1N) to be transmitted over said failed protected path segment (1W) to the protection path segment (1P); said method being characterized by the use of a tandem connection monitoring function to detect said failure and a tandem connection defect indication (RDI) to communicate the occurrence of said failure from second (NE2) to first (NE1) network element and initiating said bridging step.

13. A network element for a transmission network, said network element and associated control means being adapted and programmed to

- receive and transmit traffic signals on at least one protected path segment (1W) to a far end network element;
- receive and transmit traffic signals on at least one protection path segment (1P) to the same far end network element;
- create a tandem connection (TC1) along said protected path segment (1W);
- detect a failure on said protected path segment by means of a tandem connection monitoring function; and
- upon detection of the failure; to insert a tandem connection defect indication (RDI) into a reverse traffic signal, to bridge said reverse traffic signal to the protection path segment (1P), and to select said protection path segment (1P) to receive a traffic signal from the protection path segment (1P), said defect indication (RDI) being transmitted on the protected path segment as long as the failure persists.

14. A network management system for a transmission network, said system being adapted and programmed to

- provide at least one protected path segment (1P) between a first network element (NE1) and a second network element (NE2);
- provide at least one protection path segment between said first and second network elements (NE1, NE2); and
- upon occurrence of a failure on said protected path terminate (1W) detected and communicated by one of said network elements (NE1, NE2), to provide a new working path between said first and second network elements (NE1, NE2).

Abstract

M:N Path Protection

An 1:n or m:n path protection mechanism is provided. Rather than defining an automatic protection protocol, use is made of the existing tandem connection monitoring function, tandem connection reverse defect indication (RDI), and tandem connection trail trace identifier. Upon detection of a failure on the working path segment (1W), the occurrence of this failure is communicated to the far end node by inserting forced RDI into the tandem connection as long as the failure persists. In the case of more than one protected paths, the failed path is identified by means of the unique trail trace identifier received on the protection path. In the case of several protection paths, one network node is defined as slave node which has to follow the switch-over initiated by the master node and choose the same protection path as the master node. Preferably, a combination of two timers enables return from failure condition to normal operation.

(Figure 1)

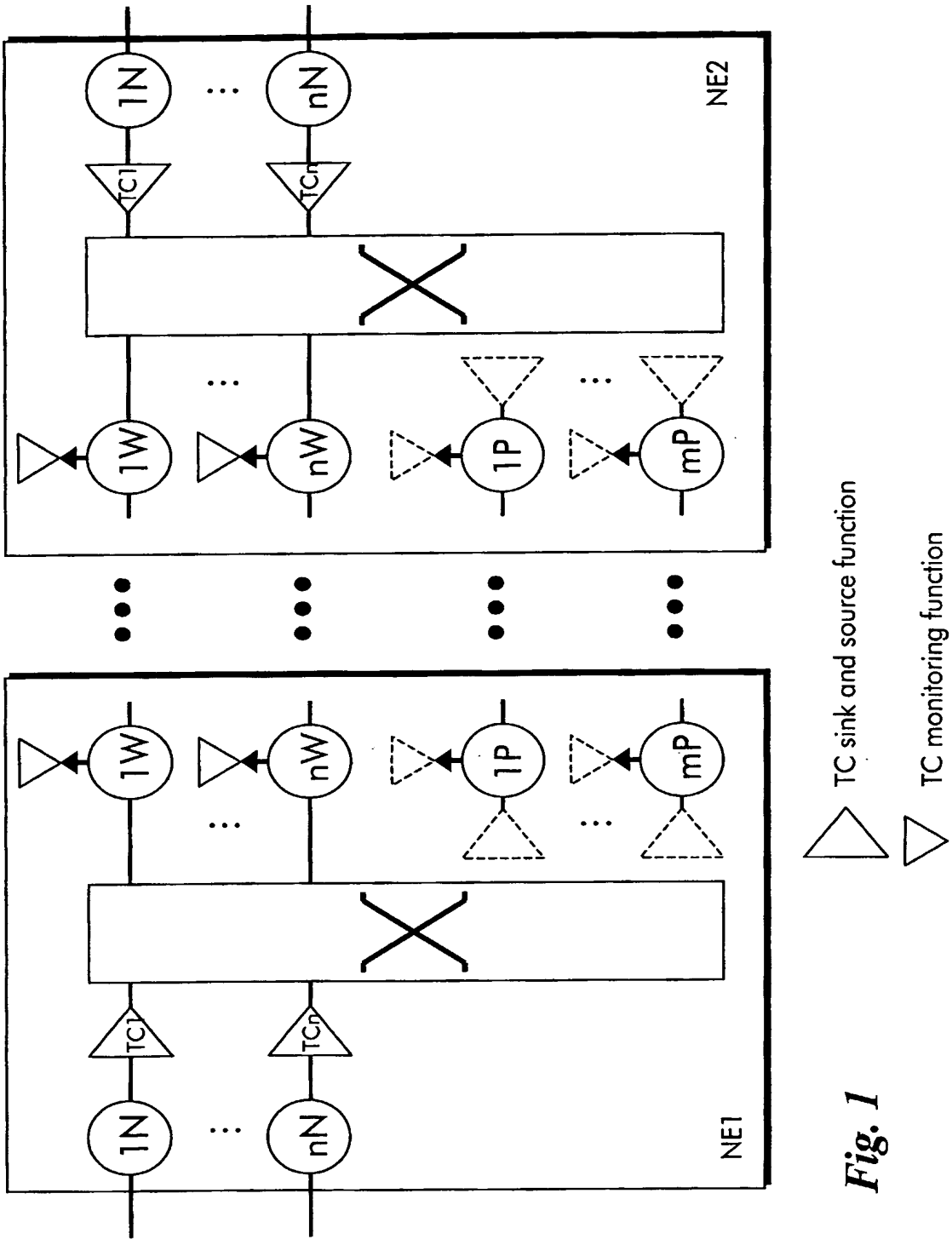
NE2
1N
nN
TC1
TCn
1W
nW
1P
mP
NE1
TC sink and source function
TC monitoring function

Fig. 1

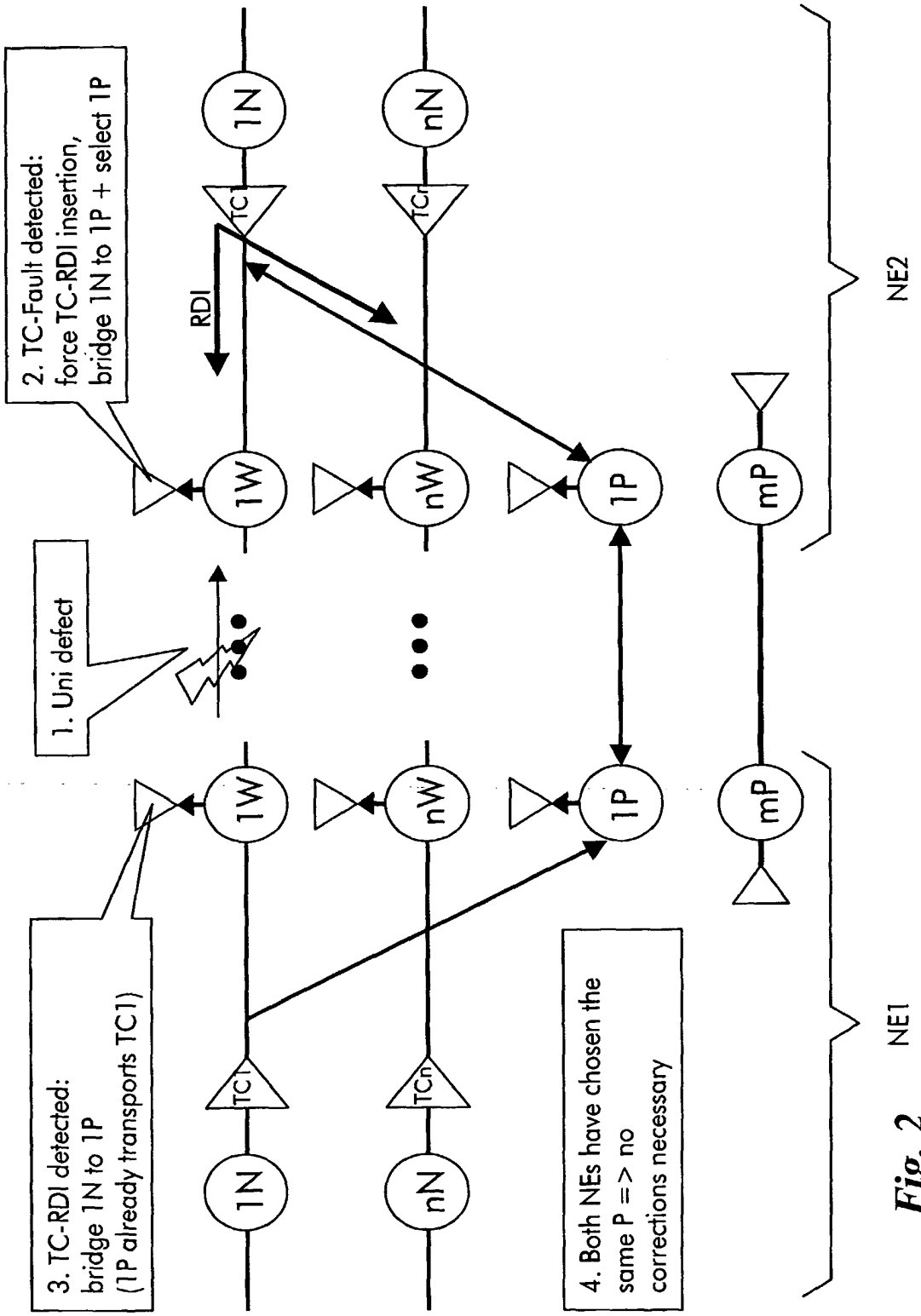
2. TC-Fault detected:
force TC-RDI insertion,
bridge 1N to 1P + select 1P
RDI
1. Uni defect
3. TC-RDI detected:
bridge 1N to 1P
(1P already transports TC1)
4. Both NEs have chosen the
same P => no
corrections necessary
1N
nN
1W
nW
1P
mP
TC1
TCn
NE1
NE2

Fig. 2

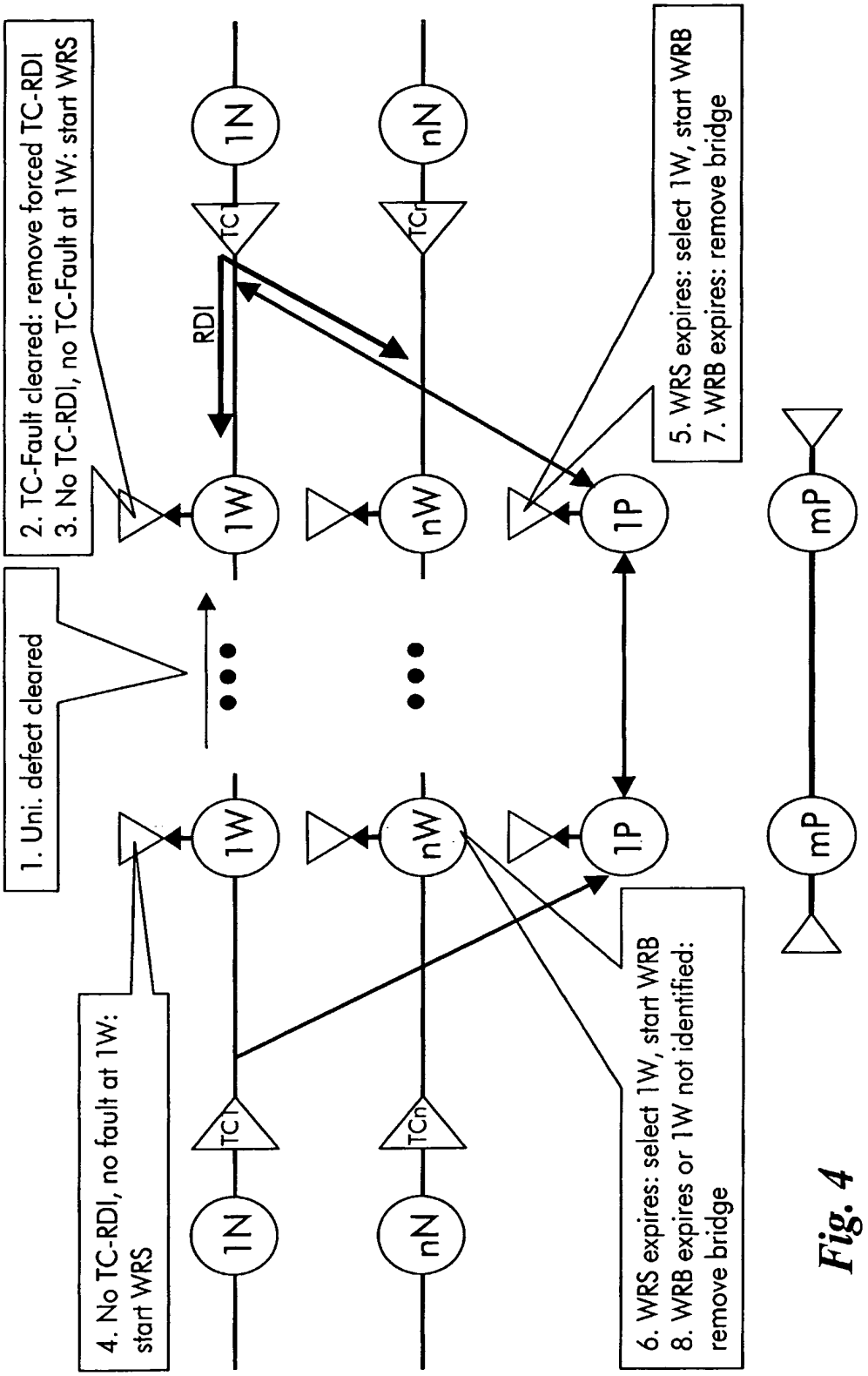
1. Uni. defect cleared
2. TC-Fault cleared: remove forced TC-RDI
3. No TC-RDI, no TC-Fault at 1W: start WRS
4. No TC-RDI, no fault at 1W: start WRS
5. WRS expires: select 1W, start WRB
7. WRB expires: remove bridge
6. WRS expires: select 1W, start WRB
8. WRB expires or 1W not identified: remove bridge
RDI
TC1
TCn
1N
nN
1W
nW
1P
mP

Fig. 4

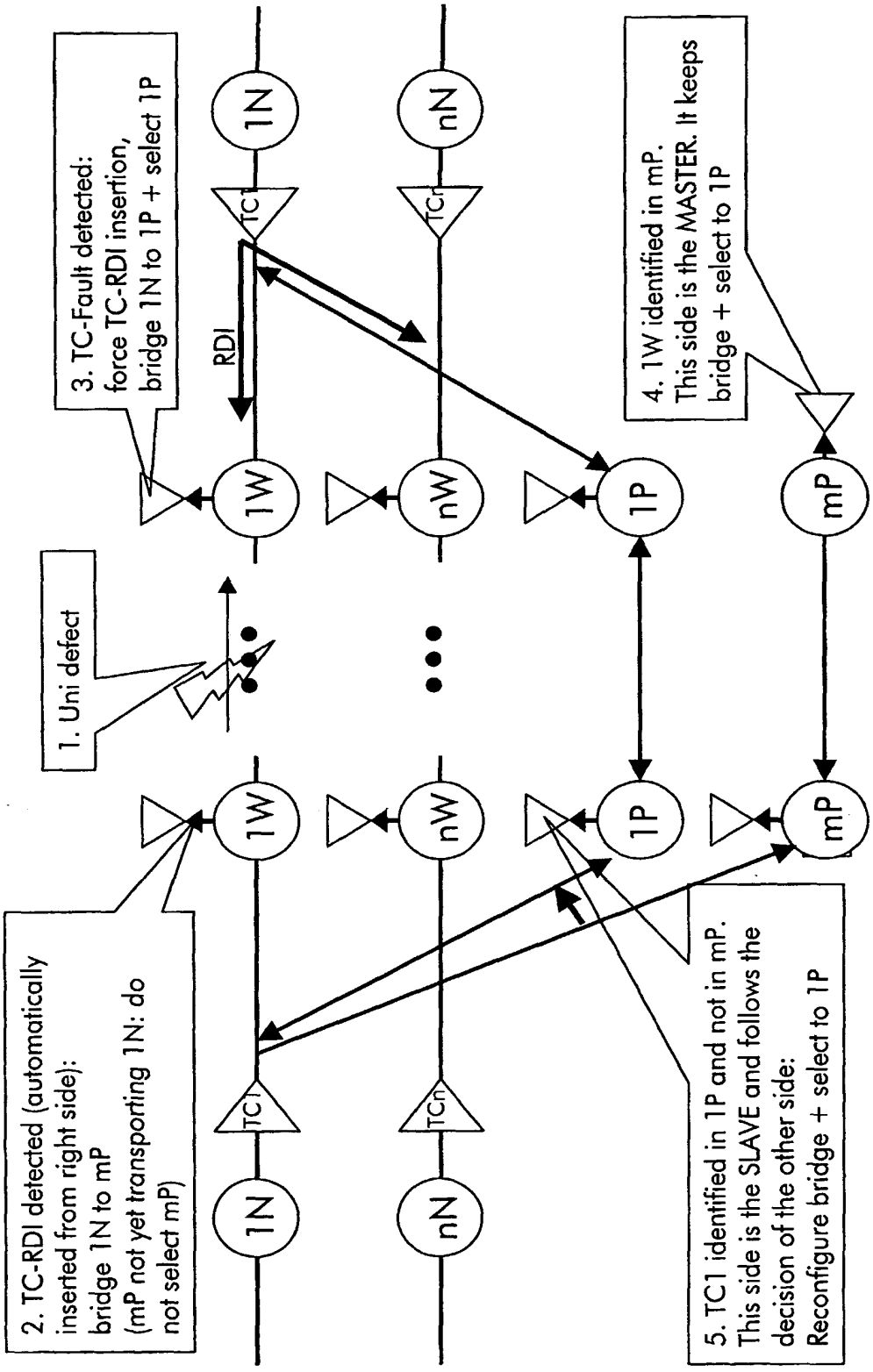
1. Uni defect
2. TC-RDI detected (automatically inserted from right side): bridge 1N to mP (mP not yet transporting 1N: do not select mP)
3. TC-Fault detected: force TC-RDI insertion, bridge 1N to 1P + select 1P
4. 1W identified in mP. This side is the MASTER. It keeps bridge + select to 1P
5. TC1 identified in 1P and not in mP. This side is the SLAVE and follows the decision of the other side: Reconfigure bridge + select to 1P
RDI
1N
nN
1W
nW
1P
mP
TC1
TCn

Fig. 3

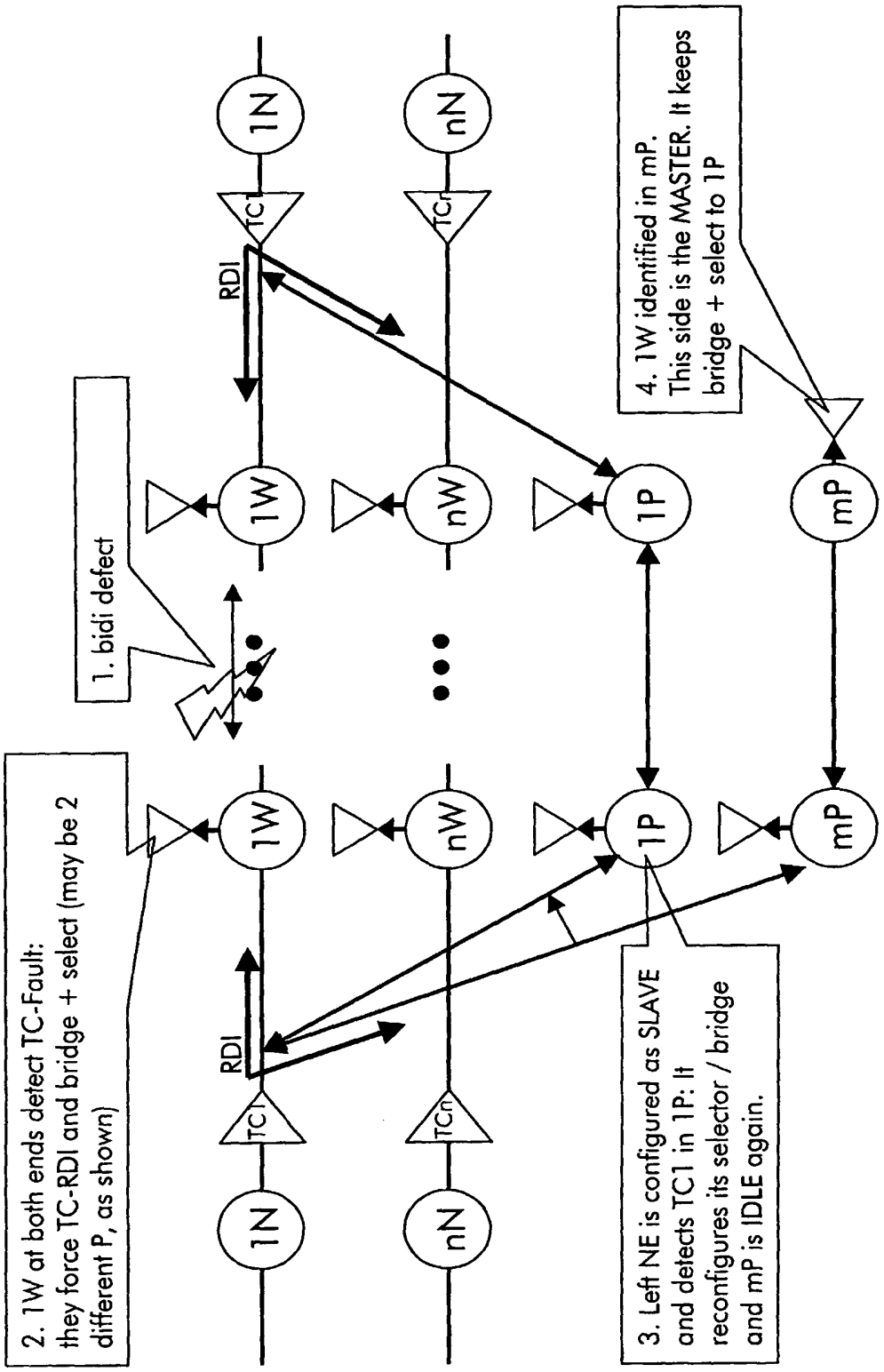
1. bidi defect
2. 1W at both ends detect TC-Fault:
they force TC-RDI and bridge + select (may be 2 different P, as shown)
3. Left NE is configured as SLAVE and detects TC1 in 1P: It reconfigures its selector / bridge and mP is IDLE again.
4. 1W identified in mP.
This side is the MASTER. It keeps bridge + select to 1P
1N
nN
1W
nW
1P
mP
TC1
TCn
RDI
RDI

Fig. 5

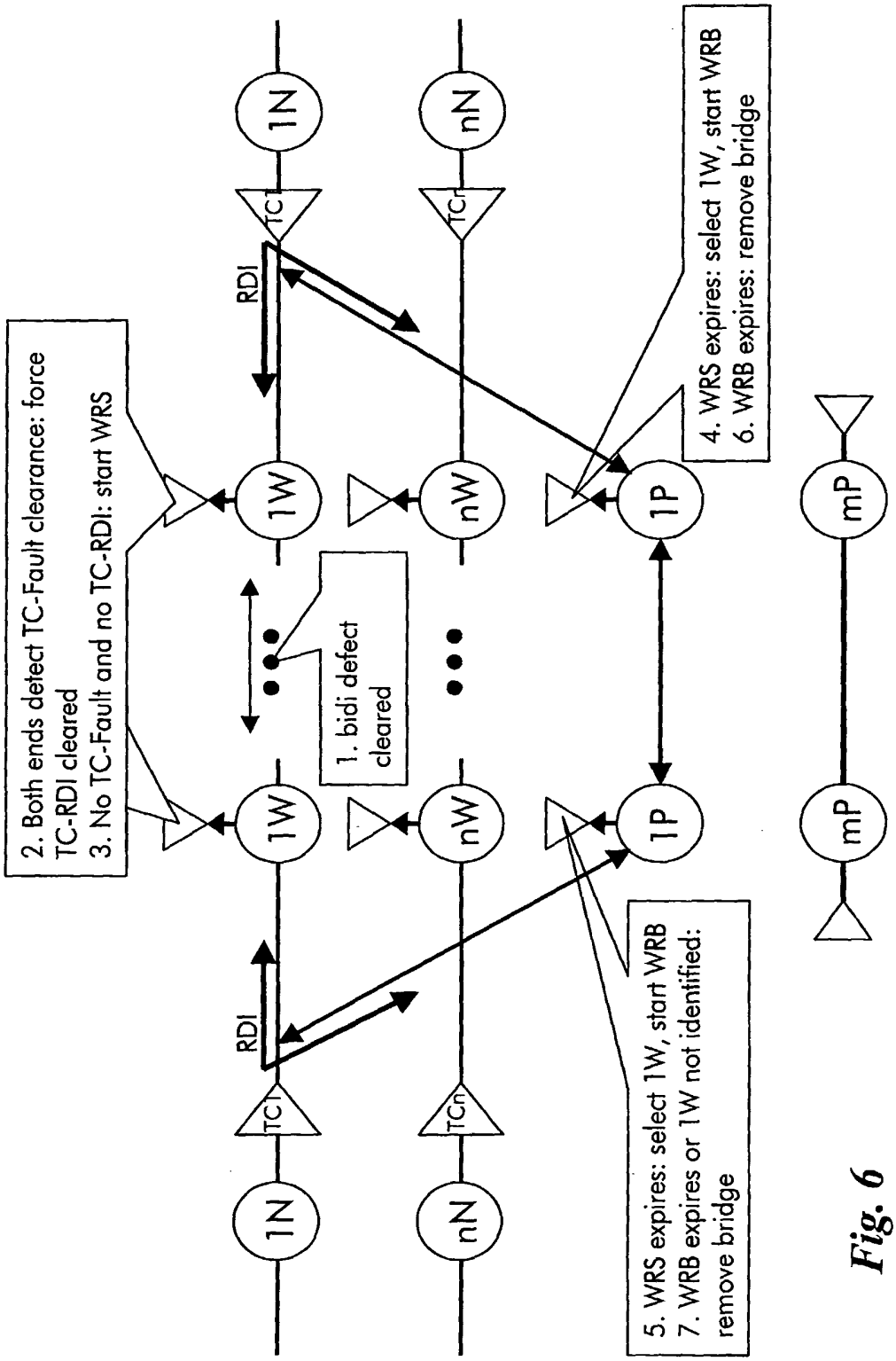
1N
nN
TC1
TCn
RDI
1W
nW
1P
mP
2. Both ends detect TC-Fault clearance: force TC-RDI cleared
3. No TC-Fault and no TC-RDI: start WRS
1. bidi defect cleared
4. WRS expires: select 1W, start WRB
6. WRB expires: remove bridge
5. WRS expires: select 1W, start WRB
7. WRB expires or 1W not identified: remove bridge

Fig. 6

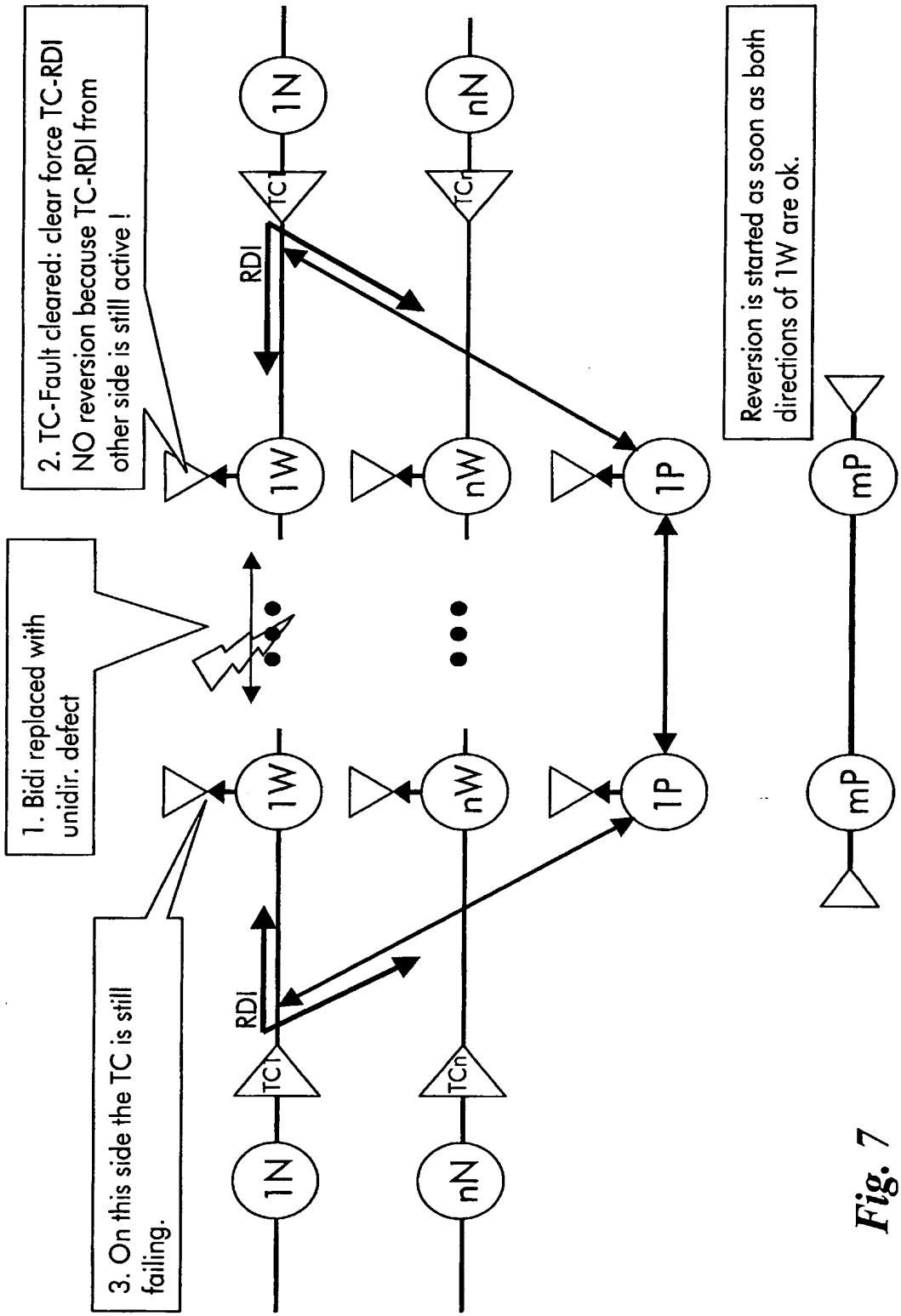
1. Bidi replaced with unidir. defect
2. TC-Fault cleared: clear force TC-RDI NO reversion because TC-RDI from other side is still active !
3. On this side the TC is still failing.
Reversion is started as soon as both directions of 1W are ok.
1N
nN
1W
nW
1P
mP
TC1
TCn
RDI
RDI

Fig. 7

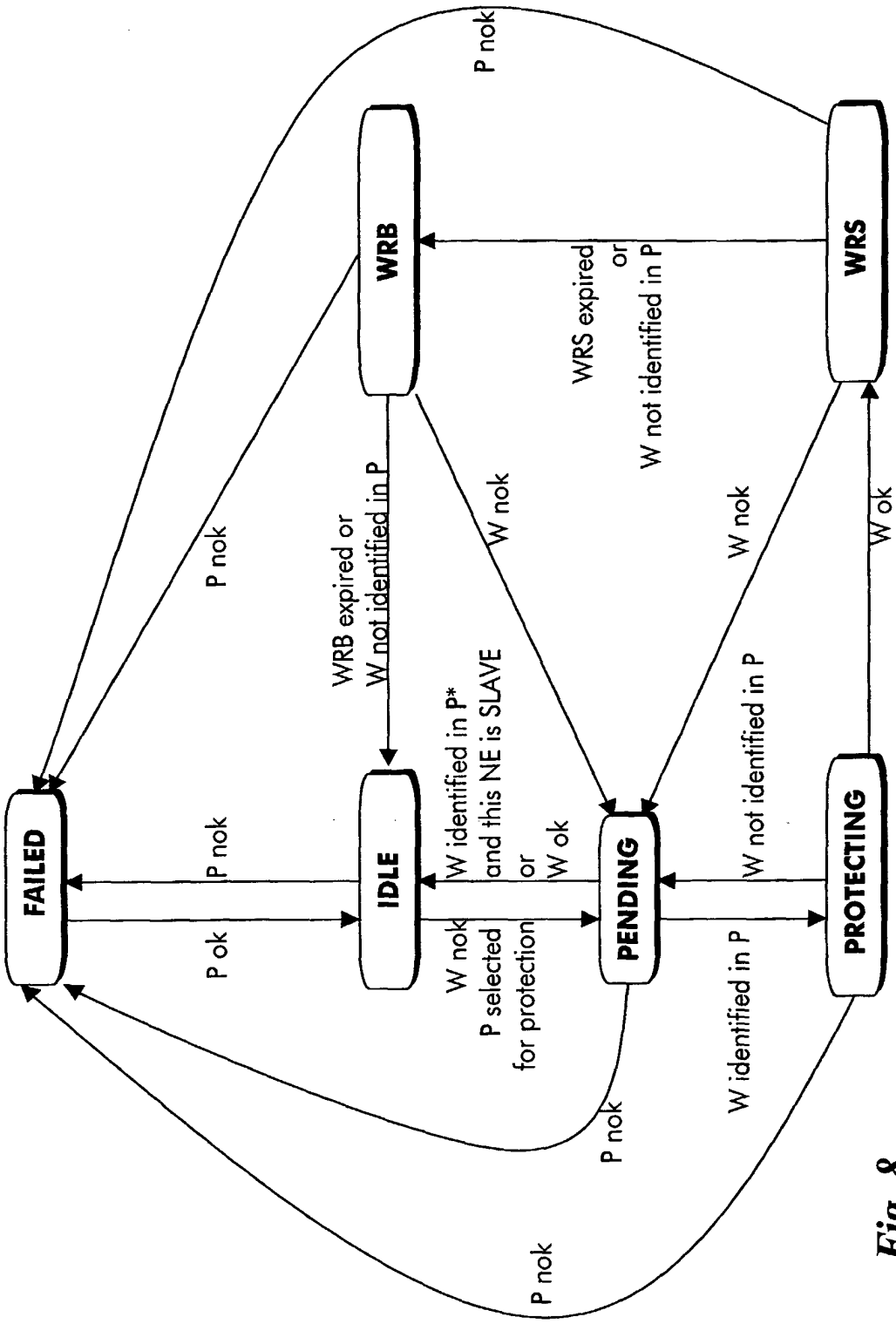
FAILED
IDLE
WRB
PENDING
WRS
PROTECTING
P nok
P ok
WRB expired or W not identified in P
W identified in P* and this NE is SLAVE or W ok
W nok
P selected for protection
WRS expired or W not identified in P
W nok
W ok
W not identified in P
W identified in P

Fig. 8

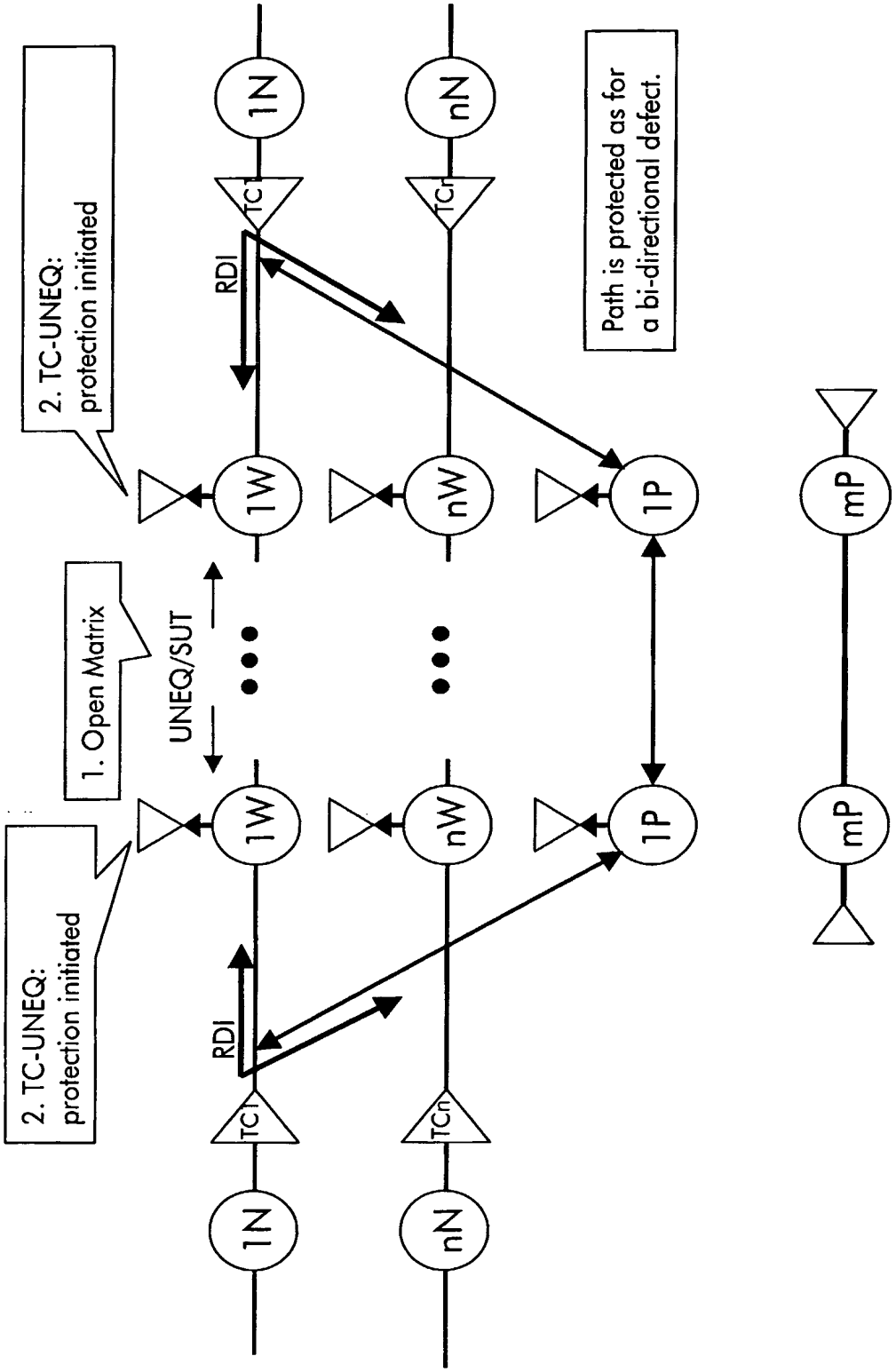
2. TC-UNEQ: protection initiated
1. Open Matrix
2. TC-UNEQ: protection initiated
UNEQ/SUT
RDI
RDI
TC1
TCn
TC1
TCn
1N
nN
1W
nW
1P
1N
nN
1W
nW
1P
mP
mP
Path is protected as for a bi-directional defect.

Fig. 10

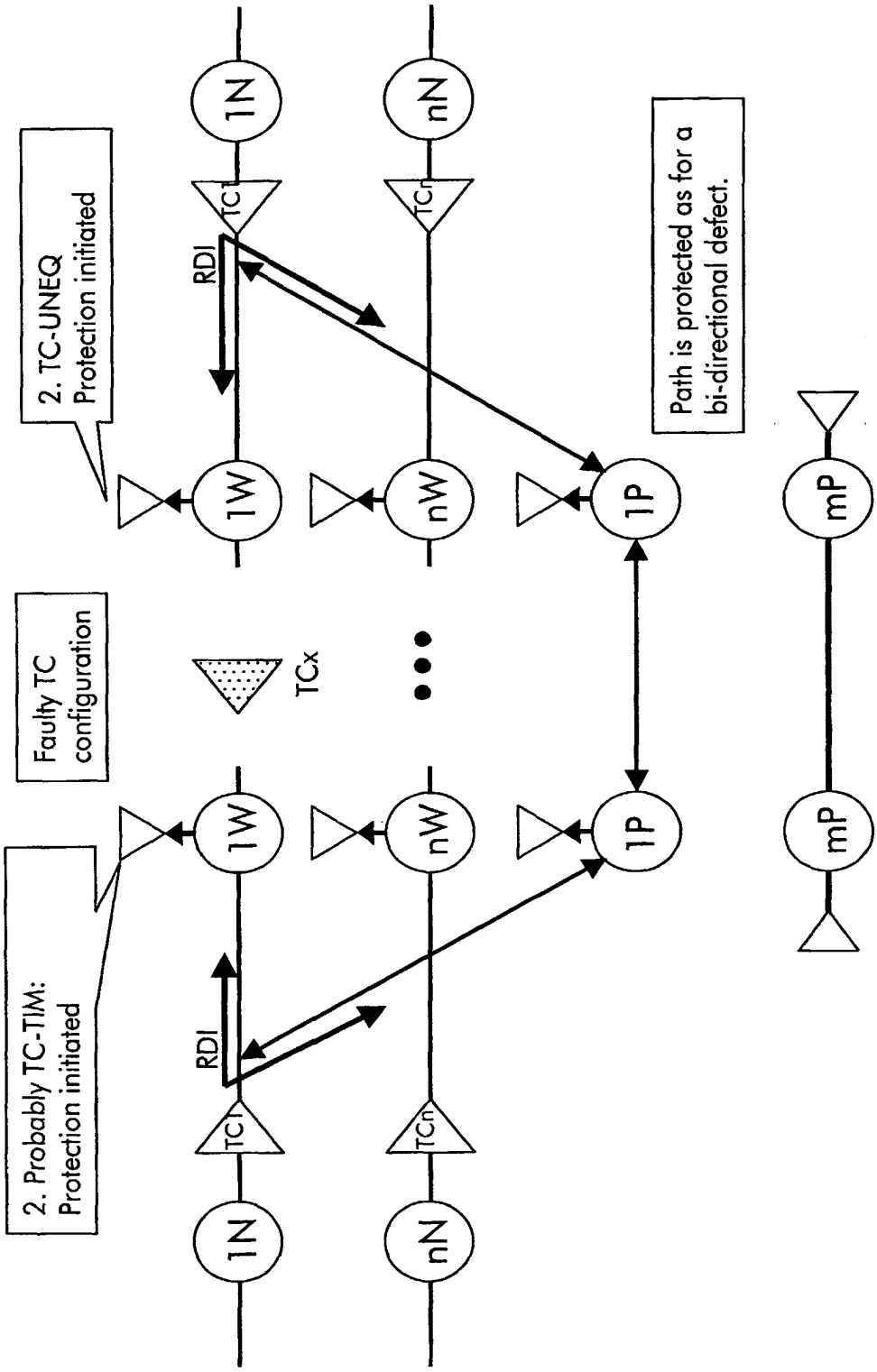
2. Probably TC-TIM:
Protection initiated
Faulty TC
configuration
2. TC-UNEQ
Protection initiated
Path is protected as for a
bi-directional defect.
1N
nN
1W
nW
1P
mP
TC1
TCn
TCx
RDI
RDI

Fig. 9

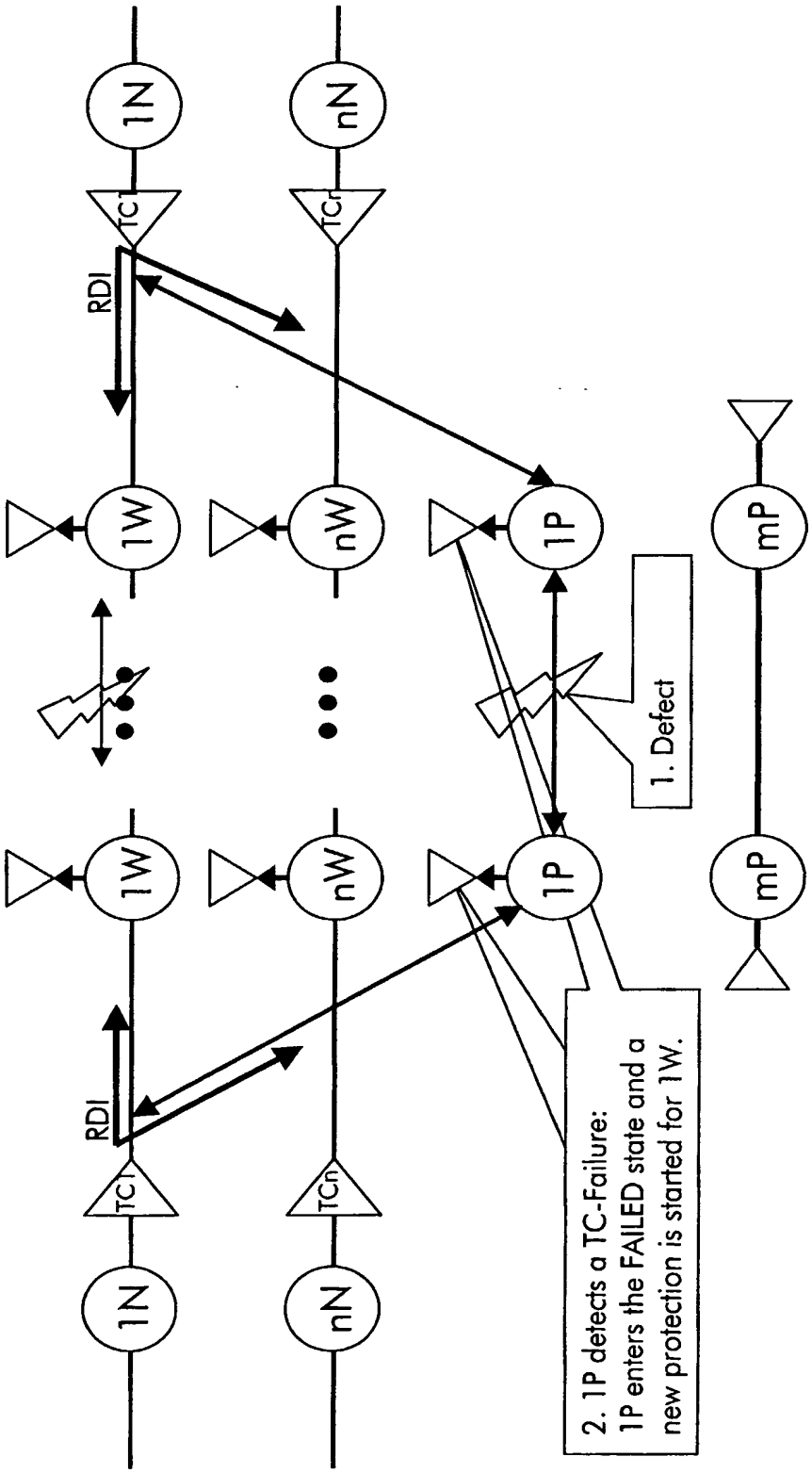
1N
nN
TC1
TCn
RDI
1W
nW
1P
mP
1. Defect
2. 1P detects a TC-Failure:
1P enters the FAILED state and a
new protection is started for 1W.

Fig. 11

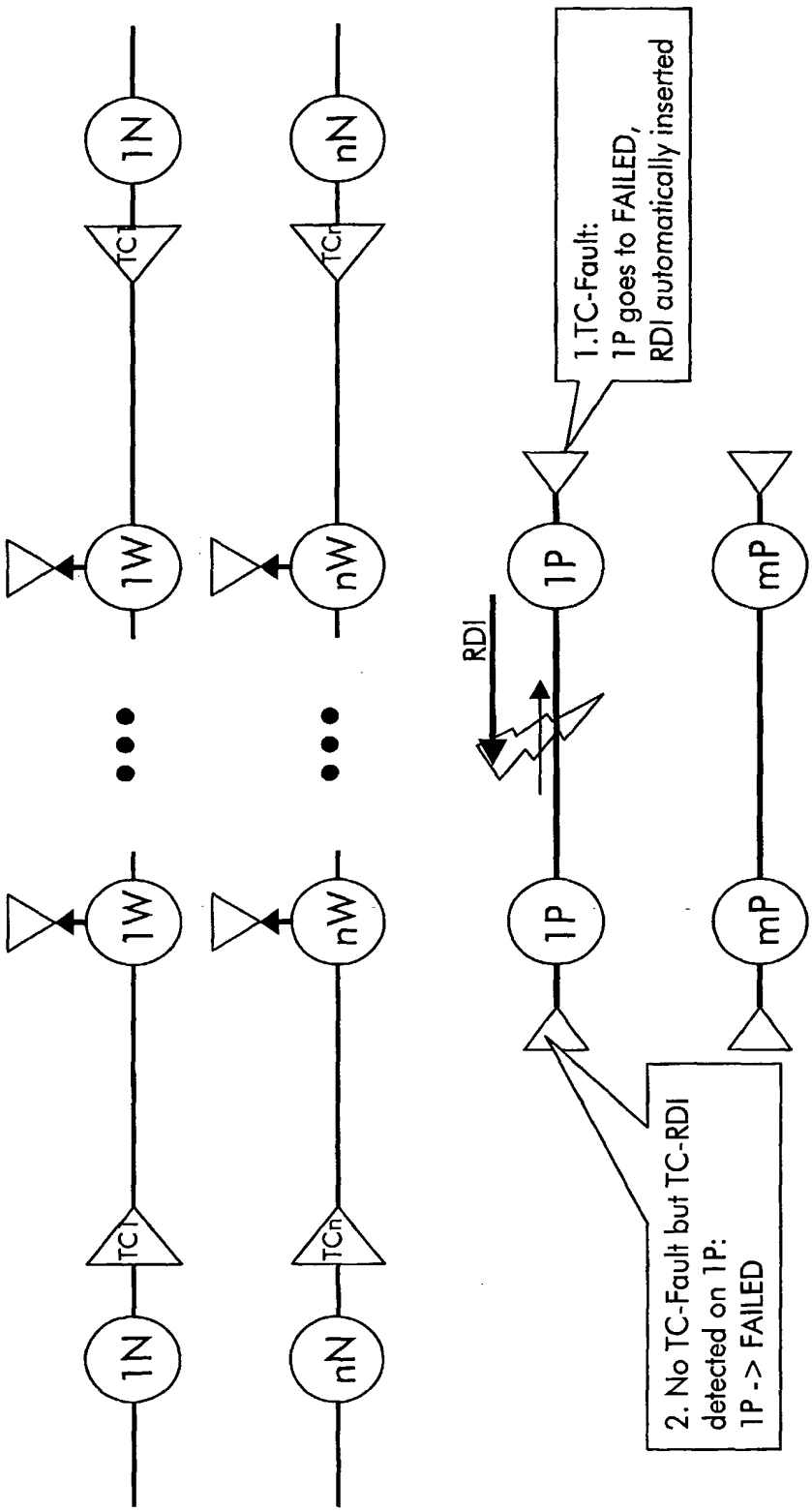
1N
TC1
1W
nN
TCn
nW
1P
mP
RDI
1.TC-Fault:
1P goes to FAILED,
RDI automatically inserted
2. No TC-Fault but TC-RDI
detected on 1P:
1P -> FAILED

Fig. 12

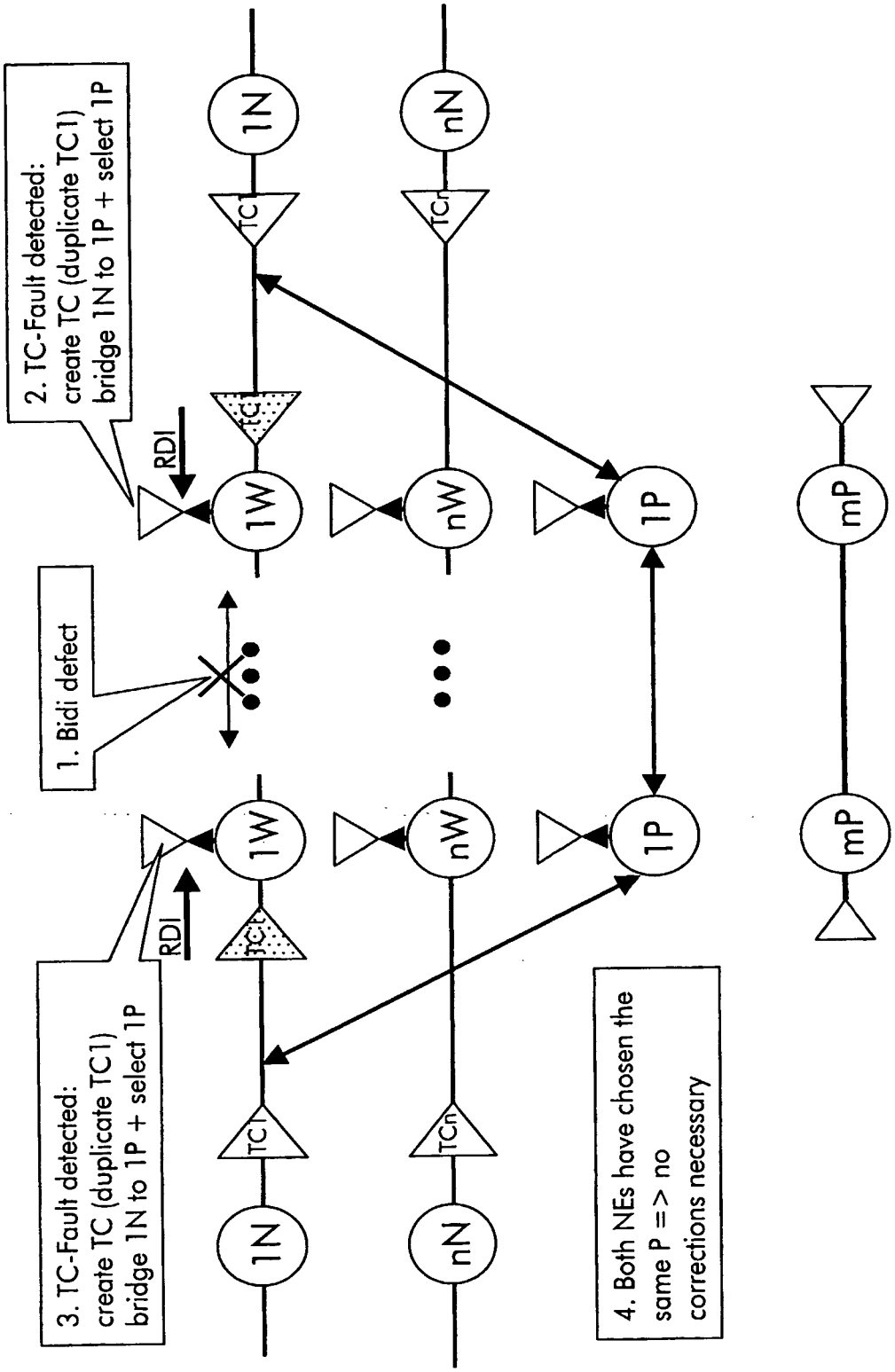
2. TC-Fault detected:
create TC (duplicate TC1)
bridge 1N to 1P + select 1P
1. Bidi defect
3. TC-Fault detected:
create TC (duplicate TC1)
bridge 1N to 1P + select 1P
4. Both NEs have chosen the
same P => no
corrections necessary
RDI
RDI
1N
nN
1W
nW
1P
mP
TC1
TCn

Fig. 13